Contribution à l'étude d'un modèle d'accident systémique, le cas du modèle STAMP : application et pistes d'amélioration

Karim Hardy

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

MINES ParisTech

École doctorale n° 432 : Sciences et Métiers de l'Ingénieur

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

l'École Nationale Supérieure des Mines de Paris

Spécialité " Sciences et Génie des Activités à Risques "

présentée et soutenue publiquement par

Karim HARDY

le 14 décembre 2010

Contribution à l'Etude d'un Modèle d'Accident Systémique

Le Cas du Modèle STAMP : Application et Pistes d'Amélioration

Directeur de thèse : **Franck GUARNIERI**

Jury

M. Benoît ROBERT, Professeur, Ecole Polytechnique de Montréal,	Rapporteur
M. Tullio TANZI, Professeur, Telecom ParisTech,	Rapporteur
M. Guy DEPELSENAIRE, Ingénieur de Recherche, Solvay S.A.,	Examinateur
M. Emmanuel GARBOLINO, Maitre Assistant, Mines ParisTech,	Examinateur
M. Franck GUARNIERI, Maitre de Recherche, Mines ParisTech,	Directeur de Thèse

T H È S E

MINES ParisTech
Centre de Recherche sur les Risques et les Crises
Rue Claude Daunesse, B.P. 207
06904 Sophia-Antipolis Cedex

Remerciements

Je tiens en premier lieu à remercier l'entreprise Solvay S.A. et tout particulièrement M. Guy Depelsenaire ainsi que l'Agence Nationale de la Recherche et de la Technologie d'avoir pu me permettre d'effectuer cette thèse CIFRE dans des conditions optimales.

Je souhaite exprimer ma gratitude aux membres du jury dont Messieurs les rapporteurs, le Professeur Benoît Robert de l'Ecole Polytechnique de Montréal et le Professeur Tullio Tanzi de Telecom ParisTech, qui ont accepté d'évaluer ce travail. Je tiens également à remercier Messieurs les examinateurs, à savoir Guy Depelsenaire de l'entreprise Solvay S.A. et Emmanuel Garbolino des Mines ParisTech, pour leur participation à ce jury.

Je remercie mon directeur de thèse, Franck Guarnieri, de m'avoir accepté au sein du Centre de Recherche sur les Risques et les Crises (CRC) des Mines ParisTech et d'avoir pris la direction de ce travail. Franck a toujours su me conseiller et être présent dans les moments délicats. Merci !

Je souhaite exprimer un grand « Merci » au Professeur Nancy Leveson, directrice du Complex System Research Lab du Massachusetts Institute of Technology, pour m'avoir permis de passer un semestre dans cette prestigieuse université en m'intégrant dans une équipe de jeunes chercheurs (Brandon, Maggie, Matthieu, John) où la production de connaissances est un défi quotidien. Nancy a su être présente et répondre à mes questions malgré ses déplacements incessants.

Merci, au personnel du secrétariat du CRC et plus particulièrement à Sandrine Renaux et Myriam Lavigne-Perrault. Elles ont su rendre la gestion de cette thèse plus

simple en s'occupant de toutes ces tâches qui nous « embêtent ». Ce travail quotidien qui peut nous paraître « périphérique » est tout simplement essentiel à la vie du labo.

Merci, à l'ensemble des personnels du CRC, les cadres et les étudiants, qui grâce à leurs travaux et à leurs enthousiasmes font avancer le labo dans une bonne direction. Je ne les citerai pas tous, pour ne pas commettre d'oubli qui pourrait vexer mais je remercie mon collègue de bureau Daniel Hummerdal pour sa disponibilité en se prêtant au jeu du débat scientifique lors de nos (tentatives d') explications théoriques.

Un « Merci » particulier et amical, au « groupe de motards », Sam, Val et Wim avec qui j'ai eu tant de discussions sur les révolutions scientifi….. Euh, non, c'était plutôt des discussions sur la mécanique et la préparation des motos. De bons et essentiels moments de détente. Je souhaite remercier également Val, Sam (encore eux) ainsi que Francis, avec qui j'ai pu m'oxygéner l'esprit grâce à nos sorties VTT autour du site de l'Ecole.

Par ailleurs, je souhaite exprimer ma plus grande reconnaissance à mes parents, qui ont su nous (avec mes sœurs) transmettre, des valeurs éducatives et familiales dénuées de tout jugement et qui font ce que je suis devenu aujourd'hui. Je suis ici aujourd'hui grâce à eux et je les remercie du fond du cœur. Ce travail est en partie le leur.

Enfin, je souhaite apporter une pensée unique pour Lorraine, qui m'accompagne dans ma vie, qui est présente tous les jours à mes côtés et qui m'apporte tant de compréhension et d'amour.

« La culture… ce qui a fait de l'homme autre chose qu'un accident de l'univers »

André Malraux

« La connaissance s'élabore contre une connaissance antérieure »

Gaston Bachelard

« La richesse du réel déborde chaque langage, chaque structure logique, chaque éclairage conceptuel. »

Ilya Prigogine

Table des matières

Introduction
— De l'idée de la thèse —

L'accident, évènement imprévisible qui cause pertes et dommages pour des populations ou encore des biens. L'accident, incident ou catastrophe, qui impose aux sociétés des changements aussi bien structurels que réglementaires. L'accident, évènement contre lequel l'homme se bat pour préserver sa sécurité et sa pérennité depuis le début de son existence… Dans des champs disciplinaires aussi variés que la philosophie, les mathématiques, la sociologie, la géographie, la médecine ou les sciences juridiques, de nombreuses recherches essaient depuis des décennies de comprendre l'accident afin de résoudre — même partiellement — des problèmes de société, d'analyse mathématique ou d'expérimentation physique ou chimique. L'accident est présent, pesant, pressant dans toute société, affectant l'ensemble des activités humaines et se traduisant par une rupture d'un continuum ou d'un état stable.

Par sa présence permanente et sournoise, l'accident, malgré une certaine acceptation sociale, fait peur, intrigue, intéresse, stimule l'être humain dans sa quête de sécurité et de survie au sein de son environnement. L'homme reste cet être doté d'intelligence qui rejette au fil des siècles toute idée de fatalité ou s'interrogeant perpétuellement sur la présence d'un être supérieur qui déciderait de sa vie ou de sa mort. Bernstein pose, par exemple, la question d'un homme plus fort que les Dieux, réussissant à maîtriser son propre destin grâce à des méthodes de gestion des risques [Bernstein, 1998].

L'accident demeure un inconnu, irrésistible, poussant les scientifiques dans des analyses et des réflexions visant à le comprendre, voire à le dompter.

Le présent travail de recherche s'intéresse à ces différentes visions de l'accident, qui cherchent à l'analyser et à l'expliquer par des démarches de modélisation dès les années 1930 et prennent une part importante dans la communauté scientifique des cindyniques.

C'est pourquoi cet ouvrage est articulé selon trois grands axes : un premier introduit l'approche dite « classique » de l'accident ainsi que ses apports et ses limites ; un deuxième décrit la vision systémique de l'accident ainsi que ses apports dans la compréhension de l'état accidentel ; enfin, un dernier axe présente l'application d'un modèle d'accident systémique appelé STAMP (*System-Theoretic Accident Modeling and Processes*) au travers d'une technique d'analyse des dangers.

Un rappel préalable des fondements scientifiques des modèles d'accident permettra néanmoins de comprendre le cadre dans lequel cette démarche s'inscrit.

La principale approche des modèles d'accident aujourd'hui connue reste déterministe et constitue le principe fondamental de toute prédiction. La raison d'être d'un modèle d'accident est en effet de pouvoir prédire, lors de l'analyse d'un système complexe (statique ou dynamique, linéaire ou non linéaire), des comportements pouvant faire migrer un système vers un état accidentel ; tous les modèles d'accident ont, depuis le modèle d'Heinrich en 1930, été développés dans un souci de compréhension et de prédiction au sein de différents types de systèmes complexes tels que des systèmes physiques ou des systèmes socio-techniques. Ces modèles d'accident se sont fondés sur une démarche déterministe, alternant approches analytiques et systémiques — aujourd'hui considérées comme complémentaires [De Rosnay, 1995]. Ces modèles d'accident considèrent implicitement que les systèmes étudiés sont des systèmes déterministes dits « intégrables ».

L'avenir est déterminé par le passé et « tout évènement est causé par un évènement qui le précède, de sorte que l'on pourrait prédire ou expliquer tout évènement. Par ailleurs, le sens commun attribue aux personnes saines et adultes la capacité de choisir librement entre plusieurs voies d'action distinctes » [Popper, 1984]. Quiconque désire prédire l'avenir et le comportement d'un système dans le futur doit observer le présent et connaître ses lois d'évolution. Ce besoin de prédiction remonte aux premiers philosophes grecs et se traduit par une démarche de compréhension d'une situation afin de prévoir son évolution et les conséquences d'une éventuelle action. Cette compréhension demande une connaissance du passé pour appréhender l'état présent ainsi que les lois d'évolution. C'est cette capacité à prédire le futur d'un évènement à partir du passé et du présent qui constitue le déterminisme scientifique. Ainsi, un système dynamique déterministe est un système prédictible. Cette vérité est illustré par le « démon de Laplace » [Prigogine, 2001], « une intelligence qui, pour un instant donné, connaîtrait toutes les forces dont la nature est animée et la situation respective des êtres qui la composent, si d'ailleurs elle était vaste pour soumettre ces données à l'analyse, embrasserait dans la même formule les mouvements des plus grands corps de l'univers et ceux du plus léger atome : rien ne serait incertain pour elle, et l'avenir, comme le passé, serait présent à ses yeux ».

Dans ce souci de compréhension, l'homme a été amené à décomposer ses observations et donc à réduire son analyse afin de se concentrer sur l'essentiel. Cet

esprit de simplification est à la base de la conception déterministe [Bachelard, 1934]. Ce réductionnisme synonyme d'approche cartésienne a permis, grâce aux travaux de Descartes, de mieux comprendre la complexité de la nature en la réduisant en des éléments simples qu'il est possible d'analyser individuellement et d'en définir des lois. Ces lois de la nature furent l'objet des recherches d'Isaac Newton et sont regroupées dans son œuvre principale, *Philosophae Naturalis Principia Mathematica*, publié en 1687. Le coup de génie de Newton a été de montrer qu'une loi appliquée à une partie d'un système pouvait aboutir à un résultat universel. Les lois de Newton ont servi de fondements à l'analyse scientifique pendant plus de trois siècles pour lesquels chaque situation, appelée « cause », a une évolution future unique, appelé « effet », prévisible grâce aux lois de la nature. Cette vision du monde déterministe met en exergue une structure parfaite, stable et équilibrée dans laquelle Dieu tient une place essentielle. L'approche déterministe est celle que l'on retrouve au sein des approches classiques et systémiques de l'accident.

La démarche de ce travail de thèse est donc organisée autour de trois grands axes. Un premier s'intéresse à l'approche classique de l'accident et permet de mettre en évidence ses limites dans un contexte de complexification des systèmes socio-techniques. Un deuxième traite des modèles répondant à ce besoin de vision globale appelés modèles d'accident systémique et illustrée par l'application d'un modèle nommé STAMP (*System-Theoretic Accident Modeling and Processes*). Un dernier axe tente d'apporter des éléments de réponse aux limites de ces approches systémiques par la prise en compte de la théorie du chaos.

L'approche « classique » de l'accident et ses limites

L'approche classique de l'accident sous-tend les modèles d'accident dits traditionnels, qui constituent aujourd'hui les modèles d'accident les plus simples et représentent une chaîne d'évènements apparaissant dans un ordre précis.

La première théorie de l'accident a été présentée par H.W. Heinrich en 1931 dans son ouvrage *Industrial Accident Prevention* [Heinrich, 1931]. Heinrich pose dix axiomes sur la sécurité industrielle pouvant être considérés, à l'époque, comme les principes fondamentaux de la sécurité industrielle. Dans ce type de modèle, l'accident est considéré comme le dernier évènement d'une chaîne d'évènements.

L'approche classique de l'accident définit le premier cadre théorique pour l'enquête accident ainsi que les évaluations de sécurité au sein des systèmes. Elle a permis de mettre au point de nombreuses techniques en sécurité des systèmes et constitue encore aujourd'hui l'approche la plus utilisée en ingénierie de la sécurité. Son influence demeure perceptible dans diverses techniques d'analyse de dangers : analyse préliminaires des risques, analyse des modes de défaillances, arbre des causes ou des conséquences… Dans ce contexte, la sécurité apparaît comme l'absence de risques au sein du système.

Cette vision linéaire et analytique de l'accident se montre très efficace pour un grand nombre de systèmes techniques mais présente au fil des années des limites dues en partie aux évolutions technologiques et à la place des facteurs humain et organisationnel [Perrow, 1984 ; Sagan, 1993] dans les causes des accidents. Par ailleurs, le caractère complexe des systèmes et la prise en compte de l'aspect dynamique des systèmes poussent les ingénieurs vers des approches plus pragmatiques. L'accident n'est alors plus considéré comme un enchaînement linéaire de causes allant d'une cause première jusqu'à l'évènement non désiré et dommageable, mais comme le résultat de nombreuses interactions opérant au sein d'un système dans lequel des éléments interagissent entre eux mais perdent à un moment ou à un autre le contrôle, faisant migrer le système vers un état accidentel. Ainsi apparaît l'approche systémique de l'accident.

La vision systémique de l'accident et ses apports possibles — Le modèle STAMP

La vision systémique de l'accident considère l'accident comme un système dans lequel des éléments interagissent entre eux afin de remplir une fonction donnée mais dont le contrôle n'a pas permis d'éviter une migration vers un état accidentel. Les modèles d'accident systémiques naissant de cette évolution reposent sur plusieurs théories qui encadrent leur application. La première — et sans conteste la plus importante — est la théorie générale des systèmes de Bertalanffy, qui dépasse l'approche analytique et considère le système comme un tout [Bertalanffy, 1968]. Cette théorie qui révolutionne littéralement l'étude des systèmes est aujourd'hui exploitée dans des domaines aussi variés que l'économie, la géographie, la biologie, la sociologie… Elle considère l'accident comme l'évènement qui provoque l'instabilité d'un système initialement stable. La seconde théorie est celle du contrôle permettant le maintien d'un système au sein de limites de fonctionnement déterminées afin d'empêcher le système de migrer vers l'accident.

L'approche systémique de l'accident a été considérablement enrichie par les travaux de Jens Rasmussen, portant sur l'analyse des accidents au sein des systèmes [Rasmussen, 1997]. Le cadre de Rasmussen permet l'étude d'un système en considérant l'aspect hiérarchique de sa structure et son aspect dynamique. L'intégration de l'aspect dynamique représente un nouveau tournant dans l'analyse des accidents et des systèmes ; elle permet la prise en compte de rétroactions aussi bien négatives que positives, créant par ce biais des comportements uniques et non linéaires au sein des systèmes.

La sécurité devient alors une propriété émergente du système et elle existe uniquement que grâce à la présence d'interactions entre éléments et à l'application de contrôles au sein de la structure hiérarchique du système.

Plusieurs modèles d'accident systémiques existent aujourd'hui, dont le modèle STAMP (*System-Theoretic Accident Modeling and Processes*) développé au

Massachusetts Institute of Technology. Ce modèle d'accident propose un changement de paradigme puisque l'accident n'est plus perçu comme le résultat d'une chaîne d'évènements mais comme la conséquence d'un problème de contrôle au sein du système. Ce modèle, articulé autour de trois concepts (la contrainte, la structure hiérarchique et le modèle de processus), constitue le pilier central de ce travail de thèse.

Vers une nouvelle génération de modèles d'accident

Les modèles d'accident systémiques fondés sur la théorie générale des systèmes de Bertalanffy — et, plus généralement, sur un cadre scientifique « newtonien » — sont d'un intérêt incontestable pour la communauté scientifique de la gestion des risques. Ils présentent cependant certaines limites, dues en partie à leur rattachement à un cadre scientifique élaboré il y a aujourd'hui plus de trois cents ans. Les modèles d'accident systémiques appréhendent souvent l'équilibre stable comme l'état « par défaut » d'un système complexe ; or, cette stabilité ne s'avère atteinte que dans des conditions très spécifiques. Cette remise en cause pousse à considérer l'instabilité des systèmes socio-techniques comme la « norme », imposant un contrôle constant afin d'éviter que le système ne migre vers l'accident.

Intégrer la dimension dynamique constitue une seconde avancée essentielle dans l'analyse des risques d'un système complexe, dont la structure est *par essence* en perpétuelle évolution. Mais prendre en compte l'évolution de processus irréversibles dans des cas *particuliers* donnerait un sens nouveau au paramètre « temps » au sein des systèmes socio-techniques : le temps ne serait qu'une constante dans un état d'équilibre stable, et une variable au sein des systèmes socio-techniques caractérisés à la fois par l'irréversibilité des processus qui s'y déploient et par leur statut de systèmes non intégrables.

La théorie du chaos permettrait vraisemblablement d'incorporer aux modèles existants ces notions d'équilibre et de temps puisque les systèmes socio-techniques, instables par essence, n'entrent qu'exceptionnellement en état d'équilibre stable.

Structuration de l'ouvrage

Cet ouvrage est organisé en deux grandes parties (figure 1).

La première partie est subdivisée en trois chapitres :

- le premier présente ce qu'est l'accident grâce à différentes définitions. Il s'intéresse également aux objectifs du processus de modélisation de l'accident dans le cadre d'une enquête accident ou d'une évaluation de la sécurité. Enfin, il développe l'approche classique de l'accident, jusque dans ses limites ;

- le deuxième chapitre s'intéresse à l'accident dans le cadre de la théorie générale des systèmes de Bertalanffy. Après avoir introduit la systémique en tant que discipline, il présente la notion d'état accidentel au sein du système ;
- le chapitre 3 présente le modèle d'accident STAMP. Ce modèle récent et encore en développement est exposé d'abord d'un point de vue fondamental, puis conceptuel. La technique d'analyse des dangers STPA (*STAMP-based Analysis*), fondée sur le modèle STAMP, est ensuite présentée.

Une deuxième partie est composée de deux chapitres :

- le chapitre 4 est consacré à l'application de la technique d'analyse des dangers STPA au sein d'un système socio-technique industriel de traitement de sédiments contaminés, en vue d'en évaluer la sécurité. Après avoir délimité les conditions de son application, il expose les résultats d'analyse enregistrés ;
- enfin, un dernier chapitre présente les limites et les apports du modèle STAMP, et évalue la technique STPA. Un changement dans la compréhension même de l'accident est ensuite proposé, en se fondant principalement sur la théorie du chaos et les travaux du prix Nobel de chimie 1977, Ilya Prigogine.

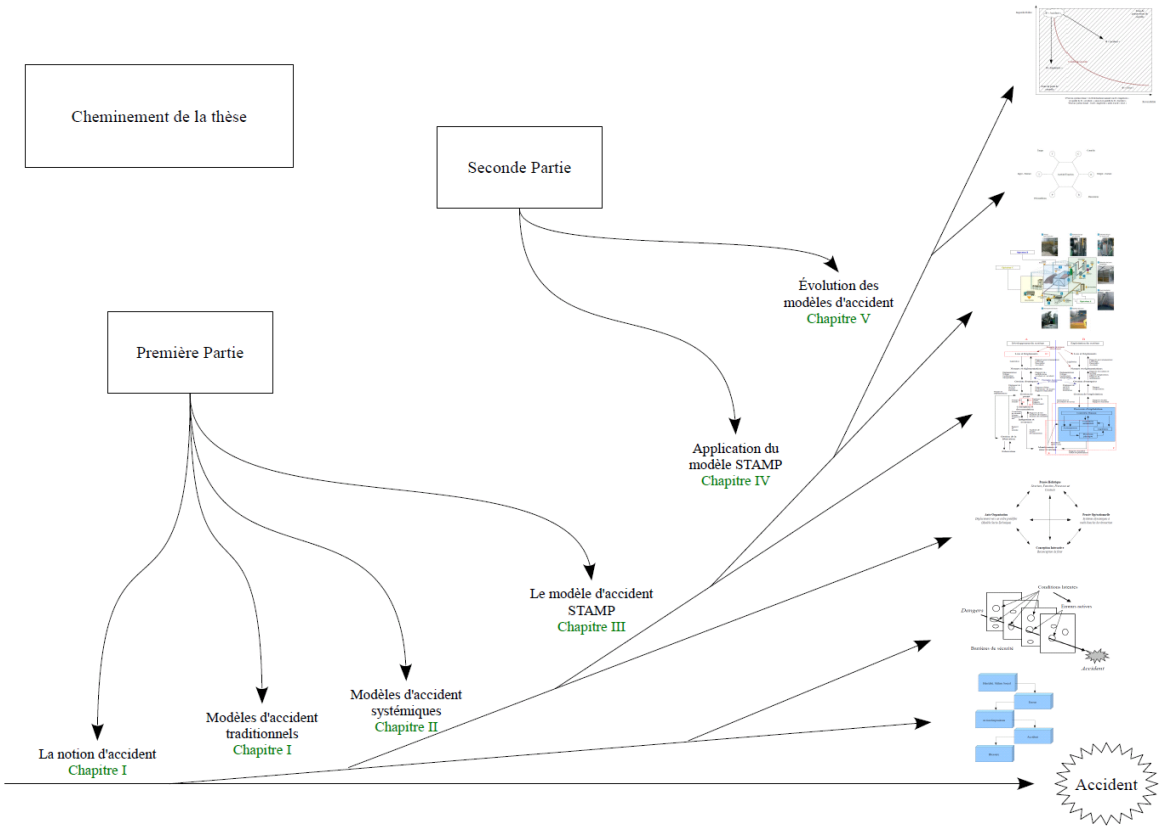


Figure 1 ■ Cheminement de la thèse
« Bifurcations » de réflexion

1re partie

Théories et modèles

Chapitre 1
Comprendre l'accident

La notion d'accident fait l'objet de définitions nombreuses dans des domaines tels que la géographie, la psychologie, la sociologie, l'histoire, voire les arts et les lettres.

Ce chapitre poursuit quatre objectifs :

- Il s'attache tout d'abord à définir la notion d'« accident » par le biais de définitions tirées d'une littérature élargie afin de présenter un éventail des différents sens du terme « accident ».
- Dans un deuxième temps, il explore les représentations et les modélisations de l'accident. Pour cela, nous décrirons brièvement les buts d'une démarche d'enquête accident pour comprendre la survenance d'un accident et ceux d'une démarche d'évaluation de la sécurité dans un souci d'amélioration de la performance.
- Puis, une troisième section présente les principaux modèles d'accident développés et décrits dans la littérature au cours du XX^{e} siècle. Ces modèles d'accident se caractérisent par des fondements et une approche linéaire qui déterminent notamment les modèles d'accident développés par Heinrich et Reason, le premier étant séquentiel alors que le second privilégie une approche organisationnelle de l'accident.
- Enfin, une présentation et des discussions seront introduites concernant deux théories organisationnelles des risques, toujours d'actualité : la théorie de l'accident normal de Charles Perrow, développée dans les années 1980, et celle des organisations de haute fiabilité (HRO), du groupe de Berkeley dans les années 1990.

Le but de cette section est de présenter certaines définitions de la notion d'accident.

1. Qu'est-ce que l'accident ?

Étymologiquement, le mot « accident » vient du latin « *accidere* » signifiant « arriver ». Ce substantif masculin désigne donc « un évènement inattendu qui survient par hasard » ou encore « un évènement impromptu causant des dégâts corporels ou matériels ».

« On ne peut comprendre l'accident. Si on pouvait le comprendre, on comprendrait aussi la façon avec laquelle on va agir. Or cette façon avec laquelle on va agir, c'est l'imprévu, on ne peut jamais la comprendre » [Bacon, 1996]. Ces propos proviennent de Francis Bacon s'adressant à Marguerite Duras en 1971 dont la réponse fut « Je ne peux le définir ». On ne peut que parler 'autour' » [Bacon, 1996] comme si la seule possibilité de vaincre « l'accident » était de le contourner comme ce peut être le cas face à un ennemi trop armé par temps de guerre.

Pour David Le Breton, l'accident est synonyme d'une dégradation, d'une érosion du destin sur l'autel des dieux. L'accident est le résultat du désordre du monde, « d'une irruption mortifère d'une série de causalités dont le hasard est le détonateur » [Le Breton, 2000].

Pour le Littré, un accident est « ce qui advient fortuitement ; un évènement malheureux ». Historiquement, le mot « accident » se retrouve dans certains écrits de Nicole Oresme, surnommé l'Einstein du XIV^{e} siècle : « Se aucun veut rendre à celui à qui il est deu son depost ou son gage, et il est contraint à non rendre, l'en doit dire que il fait injuste par accident ».

Pour Cournot, « les évènements amenés par la combinaison ou la rencontre d'autres évènements qui appartiennent à des séries indépendantes les unes des autres, sont ce que l'on nomme des évènements fortuits ou des résultats du hasard ». Quelques exemples serviront à éclaircir et à fixer cette notion fondamentale. « Il prend au Bourgeois de Paris la fantaisie de faire une partie de campagne, et il monte sur un chemin de fer pour se rendre à sa destination. Le train éprouve un accident dont le pauvre voyageur est la victime, et la victime fortuite, car les causes qui ont amené à l'accident ne tiennent pas à la présence de ce voyageur » [Cournot, 1851].

Pour Fromentin, « les seuls accidents domestiques dont j'eusse été témoin, c'étaient, pour ainsi dire, des accidents de saison qui troublaient la symétrie des habitudes, comme par exemple un jour de pluie venant quand on avait pris quelques dispositions en vue du beau temps » [Fromentin, 1863].

L'accident est aussi cet évènement pouvant entraîner la mort. Pour Ruyer, « le suicide d'un homme est un évènement essentiellement inharmonique, mais il n'est pas un évènement fortuit. Un accident comme la mort d'un homme causé par la chute d'une tuile est à la fois inharmonique et fortuit. Même si l'on admet par l'indépendance absolue des séries du hasard, il faut accorder qu'il n'est pas relatif à l'homme, puisque l'éloignement de la racine commune des deux séries, leur

fonctionnement pratiquement indépendant, est quelque chose d'objectif » [Ruyer, 1930].

Alain voit lui dans l'accident « un évènement qui apparaît comme imprévisible et improbable. Par exemple une voiture au passage à niveau juste en même temps que le train. Un obus qui enlève la tête de l'aviateur. On accuse alors la fatalité, comme si l'évènement était un défi aux lois du probable ; et cette idée a beaucoup de vrai. Le fatalisme nous console de ce qui est arrivé ; mais il ne doit pas diminuer notre prudence » [Alain, 1951].

De façon plus spécifique et d'un point de vue juridique, l'accident survenant sur le lieu de travail — plus communément appelé accident du travail — a été défini par un arrêt de la Cour de cassation en date du 21 octobre 1941 comme « une atteinte à l'intégrité du corps humain survenue par suite de l'action violente et soudaine d'une cause extérieure ». La législation des accidents du travail a pour but de protéger les salariés et assimilés contre les risques d'accidents résultant de l'exécution de leur travail.

Plus généralement, si le risque est une potentialité alors l'accident est une réalité [Le Ray, 2006]. L'accident est souvent défini comme la survenance du risque lorsque le danger touche sa cible, causant plus ou moins des dommages. C'est cette différence de dommages qui permet de porter une distinction entre un incident, un accident ou une catastrophe. Par ailleurs, alors que le risque est un non-évènement, l'accident est un évènement. Qu'il soit vu de façon statique ou dynamique, l'accident peut faire l'objet d'une démarche de modélisation visant d'une part à mieux le comprendre, d'autre part à évaluer le niveau de sécurité d'un système.

Les innovations techniques et technologiques permettent une simultanéité entraînant une grande possibilité de chocs en série. Pratiquement tout dans les sociétés industrielles et occidentalisées participe à un nouveau régime d'accident en raison d'une urbanisation grandissante, d'une multiplication des moyens de transport et de communication, de la complexification des outils et des technologies. Les catastrophes naturelles cèdent le pas aux catastrophes industrielles comme Tchernobyl, Seveso ou AZF [Métais-Chastanier, 2010].

Il semble également intéressant de souligner un renversement épistémologique dans le rapport entre l'homme et l'accident. Pour Paul Virilio, il serait trompeur d'opposer une époque durant laquelle l'homme subissait les accidents à une époque durant laquelle il pourrait participer à leur survenue. En effet, « inventer le navire à voile ou à vapeur, c'est inventer le naufrage. Inventer le train, c'est inventer l'accident ferroviaire du déraillement. Inventer l'automobile domestique, c'est produire le télescopage en chaîne de l'autoroute » [Virilio, 2005].

Ces différentes définitions de l'accident mettent en avant l'ambition qui anime certains courants de recherche cherchant à comprendre comment et pourquoi les accidents surviennent. Cette volonté s'efforce systématiquement d'expliciter l'accident en représentant le phénomène accidentel — une tentative qui peut se

traduire soit par une « enquête accident », soit par l'évaluation de la sécurité d'un système. Pour ce faire, ces démarches s'appuient sur des modèles dont l'objet peut être soit la connaissance des circonstances d'un accident, soit l'amélioration du niveau de sécurité d'un système et donc de sa performance.

Ces deux démarches font l'objet des paragraphes 2 et 3.

2. Modéliser l'accident pour le comprendre

Les modèles d'accident ont démontré leur utilité dans de nombreux domaines techniques et scientifiques en jouant un rôle essentiel dans l'analyse et la compréhension des accidents, dans la gestion des risques au sein des systèmes ou encore dans le management d'un système par la sécurité. En recourant à des outils et à des techniques spécifiques, la modélisation offre une mise en perspective novatrice par rapport à l'approche systémique classique. Un modèle permet également de préciser les éléments qu'il s'avérera utile de rechercher dans un système, en mettant en lumière certaines influences ou interactions. Enfin, l'effort de simplification induit par la modélisation conduit à ordonner le système étudié, afin d'apporter des réponses à un problème ou à un phénomène donné.

D'après Le Moigne, la modélisation est l'« action d'élaboration et de construction intentionnelle, par composition de symboles, de modèles susceptibles de rendre intelligible un phénomène perçu complexe, et d'amplifier le raisonnement de l'acteur projetant une intervention délibérée au sein du phénomène ; raisonnement visant notamment à anticiper les conséquences de ces projets d'actions possibles » [Le Moigne, 1999]. Cette définition sous-tend au moins deux notions qu'il semble nécessaire de souligner :

- d'une part, l'« élaboration et la construction intentionnelle », qui mettent en exergue l'existence d'une *représentation mentale* ;
- d'autre part, la volonté d'« anticiper les conséquences de ces projets d'actions possibles » induit la *simulation*.

Cette démarche de représentation est également présente dans le domaine de la sécurité et dans la compréhension et l'analyse des accidents. Il est important de souligner, avant de présenter différents types de modèles d'accident, qu'un modèle est *contraignant*, *limité* et, d'une certaine manière, *biaisé*, puisqu'il n'autorise à appréhender la réalité qu'à travers un prisme donné. Or, un accident — comme la sécurité d'un système dans son ensemble — peut apparaître différent lorsqu'un autre angle de vue est adopté.

Les modèles d'accident servent à étudier un accident en décrivant les relations existant entre les causes et les effets. Ils permettent d'expliquer la survenance des accidents et peuvent être également utilisés comme techniques d'évaluation des risques lors du développement et de l'exploitation d'un système. Les principaux

modèles d'accident aujourd'hui disponibles ont été développés avant que l'analyse ne prenne en compte les systèmes socio-techniques ; ils ont donc été mis à niveau mais se trouvent malheureusement dépassés par les changements technologiques rapides [Leveson, 2003].

Aujourd'hui, les modèles d'accident permettent de comprendre la survenance d'un évènement par le biais d'enquêtes dans les systèmes socio-techniques [2.1] mais servent par ailleurs d'outils d'évaluation des risques au sein de ces mêmes systèmes [2.2].

2.1. L'enquête accident

Une enquête accident consiste en la recherche des causes ayant conduit à un accident par le biais d'une représentation ou d'un modèle visant à le comprendre. Elle se fonde notamment sur les théories de l'erreur qui stipulent que dans les systèmes complexes, les erreurs des opérateurs sont les conséquences logiques d'antécédents présents dans le système au moment de l'erreur [Strauch, 2002]. Plusieurs auteurs se sont penchés sur cette notion d'erreur et ont essayé de la définir afin de mieux comprendre l'accident. Parmi eux, citons Rasmussen qui, en 1983 définit pour un opérateur trois types de performance, auxquelles peuvent être associées trois types d'erreur [Rasmussen, 1983]. Le premier et le plus simple des trois types de performance est basé sur le *savoir*, qui désigne ce qu'une personne peut acquérir au cours du temps ; le deuxième type se fonde sur la *règle*, tandis que le troisième — tenu pour le plus important par Rasmussen — considère la *connaissance*.

Un important travail sur la notion d'erreur a également été conduit par James Reason permettant de distinguer les erreurs des violations ou différents degrés d'erreur [Reason, 1990]. Il est notamment à l'origine de la notion d' « erreur latente » au sein des systèmes, que l'on retrouve dans son modèle d'accident dit du « fromage suisse ».

Cette notion d'erreur est au cœur même de l'enquête accident et pour Senders et Moray, elle désigne « quelque chose qui a été fait de façon non intentionnelle par son auteur, non désirée par les règles ou par un observateur extérieur ou menant un système hors de ses limites acceptables » [Senders et Moray, 1991]. Pour Reason, l'erreur est « un terme générique considérant l'ensemble des occasions dans une séquence planifiée d'activités mentales ou physiques ne permettant pas d'atteindre un objectif attendu » [Reason, 1990]. Pour Hollnagel, le terme « erreur humaine » est trop simpliste et il semble plus approprié d'utiliser le terme d'« action erronée » [Hollnagel, 1993]. Malgré ces différentes définitions, chacun s'accorde à dire que l'erreur pointe un résultat différent de ce qui était attendu.

Une enquête accident peut être menée pour remplir plusieurs objectifs et pour Senders et Moray, « ce qui semblait être la cause d'un accident dépend de la demande ; il n'y a pas de cause absolue » [Senders et Moray, 1991]. D'après

Rasmussen, Pejtersen et Goodstein, les enquêteurs doivent adopter une démarche visant à confronter plusieurs points de vue [Rasmussen, Pejtersen, Goodstein, 1994] — par exemple ceux de scientifiques, d'avocats, d'ingénieurs ou de spécialistes.

Bien que la méthodologie des enquêtes accident ne soit pas clairement définie, les enquêteurs s'appliquent à étudier les relations entre les causes et les erreurs d'une part, entre les erreurs et les éventuels incidents ou accidents d'autre part.

La compréhension d'un accident a considérablement évolué et la taille des systèmes étudiés s'est accrue. Cette compréhension passe par la recherche de causes, qui peut dépendre de chaque enquêteur et mener à des conclusions différentes [Dekker, 2006]. Ces conclusions proviennent en effet de représentations et de modélisations propres à chacun des enquêteurs. Cette subjectivité s'explique principalement par le fait qu'une démarche d'enquête accident repose sur des modèles d'accident distincts ou diversement exploités : les enquêteurs s'appuient principalement sur leur expérience, qui influence notablement leur lecture d'une situation donnée à partir de faits passés. C'est pourquoi deux démarches d'analyse du même accident peuvent parfois engendrer des résultats distincts sur les causes mêmes d'un évènement. Ce constat se retrouve aussi dans les démarches d'évaluation de la sécurité et des risques au sein des systèmes se basant sur des démarches de modélisation. Ces modèles d'accident font l'objet de la section suivante.

2.2. L'évaluation de la sécurité

Analyser et comprendre un accident implique de s'en approprier les tenants et les aboutissants au sein d'un système donné. Évaluer la sécurité d'un système passe également par cette phase de recherche des informations facilitant sa compréhension. Toute démarche de sécurité s'appuie donc sur un modèle d'accident, qui peut être ou non identique au modèle utilisé lors d'une enquête accident. Ce modèle sous-tend également les méthodes et les outils développés lors de l'analyse d'un accident ou d'une évaluation du niveau de sécurité d'un système.

Dans une démarche de sécurité, l'un des principaux avantages d'un modèle d'accident est de permettre le recueil d'informations sur le système étudié et, ainsi, d'anticiper sur ses états futurs afin d'améliorer sa performance. Ces informations peuvent être obtenues de façon claire et rapide avec des coûts relativement peu élevés. Le modèle d'accident est une représentation d'un système dans un souci d'amélioration de la sécurité pour un objectif précis ; les limites du système sont toutefois volontairement réduites afin qu'il soit possible d'évaluer la sécurité. Cette évaluation passe par l'analyse du comportement du système afin d'identifier, d'évaluer et de contrôler les dangers à l'intérieur de ses limites ; elle impose de tracer le périmètre de gestion des risques. Pour limiter puis analyser un système à risques, plusieurs types de modélisation peuvent ainsi être mis en œuvre [Le Ray, 2006] :

- la modélisation géographique ;
- la modélisation par métier ;
- la modélisation structurelle ;
- la modélisation produit ;
- la modélisation par systèmes et processus.

Seuls deux de ces types de modélisation sont d'utilisation plus fréquente [Deschanels, 2003] :

- La modélisation géographique, décomposant l'entreprise en éléments (bâtiments, bureaux, etc.), est principalement utilisée dans le domaine de la gestion des risques professionnels et en santé et sécurité au travail. Sa principale limite tient à son manque de pertinence pour représenter le fonctionnement et les différentes interactions au sein d'une entreprise.
- La modélisation systémique des systèmes et/ou des processus est le type de modélisation le plus adéquat pour la gestion des risques d'aujourd'hui [Le Ray, 2006]. En effet, une approche analytique montre à l'heure actuelle ses limites face à la complexité des interactions pouvant être à l'œuvre dans des systèmes de taille souvent très importante et de stabilité non continue.

Plus spécifiquement, les modèles ont toujours été une part essentielle de l'expérience humaine, notamment en méthodologie système. Avant toute prise de décision, un acteur utilise généralement des modèles afin de déterminer et de comprendre les résultats possibles.

Comme vu précédemment, les modèles d'accident possèdent deux principaux objectifs : ils sont tout d'abord destinés à comprendre les accidents passés, pour ensuite les prévenir. Plusieurs modèles d'accident ont été conçus avec des succès variés. Tous les modèles d'accident partagent le même postulat initial : tous les accidents présentent des caractéristiques communes, qui ne se cantonnent pas à des évènements « aléatoires ». Ces spécificités peuvent être utilisées par les modèles afin de ne considérer que certains évènements ou certaines conditions. Aujourd'hui, les modèles d'accident sont principalement issus du domaine de la sécurité industrielle, qui voit l'accident comme le résultat de multiples évènements formant une chaîne au cours du temps. C'est sur cette hypothèse la plus commune que reposent les modèles d'accident « traditionnels » et à partir de laquelle les accidents peuvent être expliqués comme une séquence d'évènements directement connectés au cours du temps [Leveson, 2006]. Une seconde hypothèse sous-tend ces modèles, selon laquelle la cause responsable du déclenchement de la chaîne d'évènements est unique et qu'à chaque évènement correspond une et une seule cause.

Les modèles d'accident servent avant tout de cadre commun de compréhension et de communication dans un souci d'efficacité dans la compréhension des accidents et de la sécurité. Néanmoins, un cadre commun impose une vision unique de l'accident et limite donc toute explication alternative.

D'un point de vue historique, les modèles d'accident ont fait l'objet de nombreux débats parmi les ingénieurs, les psychologues, les sociologues [Perrow, 1984 ; Ferry, 1988 ; Leveson, 1995 ; Vaughn, 1996 ; Reason, 1997 ; Rasmussen et Svedung, 2000 ; Leveson, 2001 ; Skelt, 2002 ; Hayhurst et Holloway, 2003 ; Johnson, 2003 ; Hollnagel et Woods, 2005].

Au cours de ces cinquante dernières années, trois grandes catégories de modèles d'accident se sont imposés. Ces modèles répondent aux évolutions de nos sociétés et à l'intégration de nouveaux paramètres tels que les facteurs humains et organisationnels dans l'analyse des systèmes accidents. Les deux premiers types de modèles reposent notamment sur les approches analytique et linéaire de l'analyse des systèmes et permettent la décomposition d'un système afin de mieux comprendre l'accident et/ou d'adopter une démarche d'évaluation de la sécurité. Le troisième type se fonde sur la théorie des systèmes afin d'adopter une vision holistique des accidents en mettant en exergue le phénomène d'émergence au sein des systèmes dont la sécurité fait partie.

L'objectif de la section suivante est de présenter ces deux premiers types de modèle d'accident : le modèle séquentiel et le modèle organisationnel, qui constituent l'approche linéaire de l'accident. Le troisième type fera l'objet du chapitre suivant.

3. L'approche linéaire de l'accident

La vision linéaire de l'accident relève des approches dites « analytiques » de l'accident, qui cherche à ramener un système à ses éléments constitutifs les plus simples [De Rosnay, 1975] et donc à étudier en détail les accidents et à comprendre les types d'interactions existant entre eux. Les caractéristiques d'une approche analytique sont résumées dans le tableau 1.

L'APPROCHE ANALYTIQUE
■ Isole : se concentre sur les éléments
■ Considère la nature des interactions
■ S'appuie sur la précision des détails
■ Modifie une variable à la fois
■ Est indépendante de la durée : les phénomènes considérés sont réversibles
■ La validation des faits se réalise par la preuve expérimentale dans le cadre d'une théorie
■ Modèle précis et détaillé, mais difficilement utilisable dans l'action
■ Approche efficace lorsque les interactions sont linéaires et faibles
■ Conduit à un enseignement par discipline
■ Conduit à une action programmée dans son détail
■ Connaissance des détails, buts mal définis

Tableau 1 ■ Caractéristiques de l'approche analytique
adapté de De Rosnay, 1975

Parmi les modèles d'accident fondés sur l'approche analytique, citons le modèle d'accident séquentiel considéré comme le premier modèle d'accident établi à partir des travaux d'Heinrich et le modèle d'accident organisationnel de James Reason.

3.1. Le modèle d'accident séquentiel

Ce modèle d'accident constitue le modèle le plus ancien et le plus simple résultant d'une séquence d'évènements survenant dans un ordre déterminé. Associé à cette approche, il se révèle très efficace pour expliquer l'enchaînement des faits dans les dernières minutes précédant la survenance d'un accident. Ce modèle prend bien en considération les relations de cause à effet, comme l'illustre la terminologie du « modèle d'accident en chaîne d'évènements ».

Ainsi, un modèle fondé sur une chaîne d'évènements décrit l'accident comme le dernier évènement d'une chaîne incluant plusieurs évènements ou facteurs causals interconnectés à travers une relation séquentielle. L'hypothèse sous-jacente à ce modèle est que *pour prévenir un accident il suffit de « casser » cette chaîne*. Cet axiome implique que les évènements soient directement liés entre eux et que la survenue d'un évènement est nécessaire pour que le suivant puisse se produire ; les évènements ont donc une relation linéaire entre eux. Ce modèle ne peut par conséquent décrire que des causalités linéaires et ne permet pas l'analyse de relation non linéaires.

Par conséquent, prévenir l'accident en utilisant une chaîne d'évènements implique de casser cette chaîne en éliminant les évènements ou en intervenant à un maillon de la chaîne. Plusieurs chaînes peuvent être également connectées ; les relations entre les évènements sont alors régis par des opérateurs logiques de type « et » et « ou ». La sélection des évènements inclus dans la chaîne se révèle arbitraire puisqu'elle dépend du domaine de connaissance de l'analyste ; la cause de l'accident dépend quant à elle de l'endroit même où la chaîne a été stoppée, ce qui peut dépendre des normes ou encore des préférences de l'analyste. Le premier évènement de la chaîne est appelé « évènement racine » ou « évènement initiateur ».

L'exemple le plus célèbre de modèle séquentiel est la théorie des « dominos » qu'Heinrich proposa en 1931 [Heinrich, 1931]. Selon ce modèle, qui constitue l'un des premiers modèles d'explication de l'accident, les évènements menant à un accident forment une rangée de dominos. En d'autres termes, l'accident est décrit comme une chaîne d'évènements survenant selon un ordre particulier.

Lorsqu'un domino chute, l'évènement suivant apparaît. Cette théorie distingue cinq facteurs dans une séquence accidentelle :

- l'environnement social,
- la faute d'une personne ou l'erreur,
- des conditions non sûres ou des actes imprudents,
- l'accident,
- la blessure.

Un évènement indésirable ou attendu déclenche la séquence des évènements sous-jacents menant à l'accident. L'accident est donc perçu comme le résultat d'une unique cause susceptible d'être identifiée et éliminée pour éviter la répétition de l'accident. Or, dans la réalité, les accidents ne sont jamais dus à un unique facteur déclenchant.

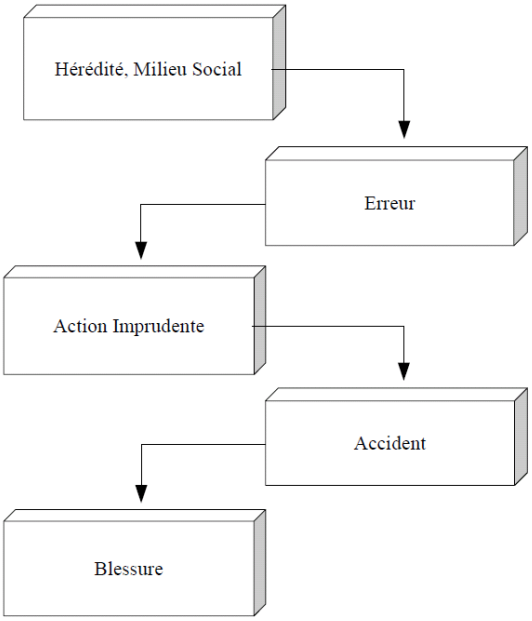


Figure 2 ■ Théorie des dominos
adapté d'Heinrich [Heinrich, 1931]

Les différents dominos représentent des facteurs d'accident formant une séquence d'évènements où le lien entre la cause et l'effet est simple. Cette théorie est le premier modèle de causalité des accidents permettant de mettre davantage l'accent sur l'erreur humaine [Hollnagel, 2004]. La simplicité de ce modèle a contribué à le rendre populaire mais c'est cette simplicité qui restreint son utilité dans le cadre des enquêtes sur les accidents dans les systèmes socio-techniques, dont il ne peut rendre compte.

Les modèles traditionnels d'accident ont été développés à partir des années 1930 pour des systèmes mécaniques dans lesquels les défaillances des éléments apparaissent de façon aléatoire et pour lesquels les redondances s'avèrent très efficaces pour réduire les probabilités d'occurrence de certaines défaillances. Ces techniques ont ensuite été utilisées dans les systèmes électromécaniques incluant des dispositifs comme des relais, des moteurs et des matériels électriques ayant une disposition pour les défaillances « aléatoires ». Ces modèles sont donc relativement performants dans le cas de pertes causées par des défaillances d'éléments physiques ou humains dans des systèmes relativement simples. Avec le développement des systèmes numériques et des logiciels, la complexité des systèmes s'est si fortement accrue que la modélisation directe des relations entre les différents éléments est devenue très difficile. Néanmoins, bien que les méthodes construites à partir des défaillances des éléments présentent un certain succès, elles continuent d'être utilisées en ignorant les relations indirectes et les impacts des logiciels sur la sécurité du système ou en assignant simplement une probabilité à une défaillance logicielle — alors que les dysfonctionnements logiciels n'apparaissent jamais aléatoirement. En effet, les logiciels ne peuvent être défaillants : ils sont programmés d'une certaine

façon et ne peuvent contribuer à un accident que si les exigences logicielles étaient fausses ou si les programmeurs y ont intégré des erreurs.

Outre cette prise en compte des logiciels, les modèles traditionnels sont limités dans la prise en compte des facteurs organisationnels affectant la sécurité du système tels que la pression managériale, les ressources limitées ou l'indépendance des décisions de sécurité.

Les méthodes fondées sur les évènements ont parfois tenté d'intégrer les facteurs humains et organisationnels. Par exemple, Elisabeth Paté-Cornell de l'Université de Stanford a inclus des facteurs humains et managériaux au sein de la méthode PRA [Paté-Cornell, 1990, Paté-Cornell, 1996] pour déterminer les probabilités de défaillance de ces systèmes. Cependant, ces travaux ne prennent pas en considération l'aspect dynamique d'un système ainsi qu'une éventuelle migration du système vers un état dangereux. La prise en compte de ces facteurs organisationnels a fait l'objet de nombreuses études et publications que le paragraphe suivant [3.2.] présente brièvement afin de comprendre cette évolution des différentes théories d'analyse des risques au sein des organisations.

Dans un modèle d'accident séquentiel, le premier évènement de la chaîne est défini comme l'évènement initiateur ; or, la sélection de cet évènement dans la chaîne est arbitraire et d'autres évènements pourraient toujours être ajoutés [Leveson, 2001]. Un évènement en particulier peut être désigné comme la cause parce qu'il se situe juste avant un accident. Dans le cas de l'accident des deux hélicoptères BlackHawk américains en Irak [AAIB, 1994], l'évènement initiateur pourrait être l'action des pilotes de F15 sachant que l'évènement précédant l'accident était le tir des missiles. Cependant, le rapport d'accident montre qu'il existait un grand nombre de causes ayant contribué à l'accident. Cette volonté de n'attribuer qu'une seule cause à un accident tire souvent sa justification dans la nécessité de désigner un responsable. Un enquêteur peut parfois s'arrêter sur une explication qui lui est familière afin de décrire et expliquer un accident. En général, il n'y a pas de critère de distinction entre les différents facteurs permettant de déterminer la « vraie » cause d'un accident [Leveson, 2001].

Il semble important de noter que le modèle d'accident séquentiel intègre la plupart des méthodes utilisées aujourd'hui, comme l'arbre des défaillances ou l'arbre des causes. Ces méthodes fonctionnent néanmoins relativement bien en cas de défaillance physique ou humaine dans des systèmes simples. Dans ce type de modèle, les causes des accidents n'étant pas qualifiées de techniques sont désignées comme des erreurs humaines [Hollnagel, 2001].

Les modèles d'accident séquentiels considèrent que la relation de cause à effet entre des évènements consécutifs est de nature linéaire et déterministe. Dans ce cadre, un accident peut montrer qu'une cause A mène à un effet B dans une situation particulière alors que A peut être la composition de plusieurs causes [Hollnagel, 2001]. Ainsi, ces modèles ne peuvent pas expliquer de façon claire les raisons d'un accident dans les systèmes socio-techniques modernes dans lesquels de nombreux

facteurs entrent en jeu et pouvant mener à des défaillances systémiques, voire à des accidents. Pour répondre à cette problématique, un nouveau type de modèle a été développé, qui tient compte des nombreuses et diverses interactions entre les éléments d'une organisation complexe.

3.2. Le modèle d'accident organisationnel

Dans les systèmes socio-techniques contemporains, les opérateurs interagissent avec la technologie en produisant des résultats issus de ces interactions. Ces systèmes composés d'hommes et de machines font partie de systèmes socio-techniques. La théorie socio-technique stipule que les hommes et les institutions sociales font partie intégrante des systèmes techniques et que pour atteindre un objectif organisationnel, il est nécessaire d'optimiser aussi bien le système technique que le système social [Trist et Bamforth, 1951]. Par conséquent, l'analyse des systèmes complexes pousse à comprendre les interactions entre les aspects technique, humain, social et organisationnel d'un système.

Dans les années 1980 est née une seconde génération de modèles d'accident, de type organisationnels (ou épidémiologiques) décrivant un accident comme la dispersion d'une maladie, c'est-à-dire comme la combinaison de facteurs présents à un moment et dans un espace donnés. S'attachant à expliquer la cause des accidents dans les systèmes complexes, cette génération de modèles diffère de la première génération sur quatre points [Hollnagel, 2004] :

- la notion de déviation de performance, qui est préférée au terme d' « erreur humaine » ;
- les conditions environnementales pouvant mener à la déviation de la performance ;
- les barrières permettant de prévenir les conséquences inattendues et pouvant stopper le développement d'un accident ;
- Enfin, les conditions latentes, constituant la caractéristique la plus importante de cette seconde génération.

Un des principaux contributeurs à cette génération de modèles d'accident est James Reason. Au début des années 1990, il élabore un cadre théorique capable de décrire et d'expliquer les accidents, et crée le terme d'« accident organisationnel » ou d' « erreur organisationnelle » [Reason, 1995 ; Reason, 1997]. Pour Reason, un accident organisationnel n'est pas dû à une simple erreur humaine et provient plutôt des interactions entre plusieurs facteurs à différents niveaux d'une organisation. Il décrit les accidents comme le résultat de plusieurs facteurs de causalité qui se combinent pour créer une « trajectoire d'accident » [Reason, 1997] à travers les multiples défenses d'un système. Selon Reason, les accidents sont le résultat de défaillances actives ou latentes se produisant au sein de cinq couches d'une organisation : les décideurs, les chefs directs, les préalables psychologiques et les activités de production et de défense. Par ailleurs, l'accident organisationnel est

défini comme une situation dans laquelle des conditions latentes combinées à des évènements locaux et à des défaillances actives commises par des opérateurs mènent à un accident.

Reason définit sa démarche comme un « modèle général afin de suivre les causes premières des différents accidents aux erreurs organisationnelles (défaillances latentes) apparaissant dans les niveaux supérieurs de n'importe quelle organisation » [Reason, 1995]. Le modèle, relativement simple et facile à appliquer, a été rapidement adopté notamment par l'industrie aéronautique. Le modèle a également été exploité par l'administration de l'aviation fédérale américaine[1] afin de mener des enquêtes sur le rôle des stratégies de management et des procédures dans les accidents et les incidents d'aéronefs. Selon Reason, ces accidents apparaissent lorsque « les trous des multiples couches sont alignés ». En réalité, les trous sont vus comme des évènements au niveau de chaque couche et ce modèle permet donc de visualiser une chaîne d'évènements.

Pour Reason, l'erreur humaine est inévitable et il est donc nécessaire de placer des défenses entre les actions humaines et les conséquences néfastes pouvant résulter de ces actions [Reason, 1997]. Cependant, prévenir les risques en identifiant les sources d'erreurs humaines (déviances de performance) et mettre en place des défenses en profondeur n'a pas permis d'empêcher certains accidents dans des systèmes complexes tels que Bhopal, Walkerton, Columbia. Les contraintes sont en effet telles que les exploitants travaillent en dehors des règles établies. De plus, la défense en profondeur pose un problème car la situation réelle du système dépend de l'intégrité et du bon état de fonctionnement de ces défenses. Ainsi, des notions telles que les défenses, les barrières ou des protections de sécurité prennent une place centrale dans l'approche de la sécurité dans les systèmes complexes. Ces défenses et couches de défense permettent de protéger le système de l'accident. Or, les défenses peuvent se détériorer au cours du temps ; ainsi, le mauvais état de fonctionnement des sprinklers est-il responsable de l'accident de la plateforme Piper Alpha [Reason, 1997]. Ce problème est également survenu lors de l'accident de Tchernobyl durant lequel les différentes couches de défense ont été supprimées pour que les opérateurs effectuent leurs tests pour un nouveau générateur. Ainsi, un trou dans les défenses peut être dû soit à une défaillance active soit à des conditions latentes. Les *défaillances actives* ou *erreurs actives* sont les actes non sûrs effectués par les opérateurs directement en contact avec le système. Ces erreurs peuvent avoir un impact plus ou moins direct sur l'intégrité des défenses. À Tchernobyl, les opérateurs ont violé les procédures et désactivé les systèmes de sécurité, menant à l'accident.

Les *conditions latentes* sont des situations pathogènes permanentes au sein du système. Elles proviennent des décisions prises par les décideurs, les concepteurs, les managers… Ces décisions peuvent être incorrectes. Les conditions latentes peuvent avoir deux effets néfastes : le premier est d'être traduit en erreur provoquant

1 FAA : Federal Aviation Administration

certaines pressions sur le système ; le second est de provoquer des faiblesses dans les défenses du système. Contrairement aux erreurs actives, les conditions latentes peuvent être gérées avant d'être traduites en erreur.

James Reason mena un grand nombre de recherches sur la recherche de ces conditions latentes notamment dans l'étude de l'accident de Three Mile Island, de la catastrophe de Bhopal ou encore pour l'accident de Tchernobyl.

Dans le modèle de Reason (figure 3), les conditions latentes et les erreurs actives sont reliées au management, considéré comme une séquence linéaire d'évènements, ce qui peut conduire à penser que la cause des accidents est une question de management organisationnel.

En 1999, Johnson et Botting utilisent le modèle de Reason pour comprendre les aspects organisationnels de l'accident de train de Watford [Johson et Botting, 1999]. Ils étudient les conditions latentes ayant contribué à la défaillance active du conducteur de train ayant provoqué la violation de deux jeux de signaux. De nombreux facteurs organisationnels ont été identifiés comme participant à la probabilité de l'accident. Malheureusement, le modèle n'a pas pu expliquer clairement comment ces facteurs ont pu mener à l'accident. La principale conclusion est que le modèle de Reason ne permet qu'une analyse d'ensemble — et non une analyse détaillée — des facteurs impliqués dans un accident.

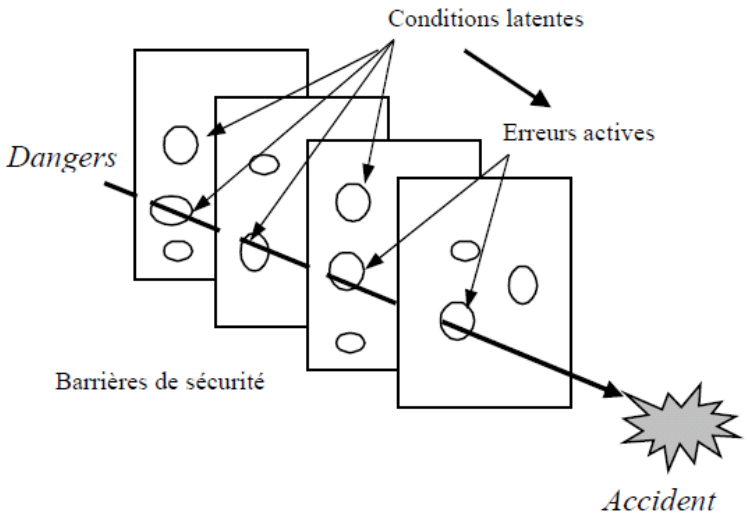


Figure 3 ■ Modèle d'accident – Fromage Suisse
adapté de Reason [Reason, 1997]

Les modèles d'accident organisationnels adoptent une vision linéaire des causes d'un accident. Le modèle de Reason constitue pour sa part une approche statique de l'accident et de l'organisation alors que le système socio-technique est beaucoup plus dynamique que ce modèle ne le suggère.

Au regard de la complexité des systèmes et de la prise en compte des facteurs organisationnels dans le rôle qu'ils peuvent jouer dans les accidents de toute nature,

il semble important de comprendre ce que peut être une théorie du risque organisationnel. En effet, le modèle développé par Reason fait notamment suite aux travaux qui ont été menés de façon préalable ou en parallèle par Charles Perrow et sa théorie de l'« accident normal » ainsi que les travaux du groupe de Berkeley dans le domaine des HRO. L'objectif du paragraphe suivant est de présenter ces deux approches organisationnelles.

3.3. La vision « organisationnelle » de l'accident

Deux courants théoriques ont principalement focalisé leur attention sur les aspects organisationnels de la sécurité : la théorie de l'accident normal [Perrow, 1999] et la théorie sur les organisations à haute fiabilité (HRO) [Rochlin, Roberts, La Porte 1987 ; Weick 1987, 1993, 1999 ; Roberts, 1990]. Bien qu'elles se soient développées simultanément, dans un contexte marqué par de forts développements technologiques, ces deux écoles divergent sur certains points, comme le montrent les deux paragraphes suivants.

3.3.1. La théorie de l'accident normal

L'approche de Charles Perrow permet de comprendre les causes des accidents dans les organisations complexes intégrant des technologies de pointe telles que centrales nucléaires, installations pétrochimiques, avions, bateaux, engins spatiaux ou armes nucléaires.

La théorie de l'accident normal développée par Perrow a été formulée à la suite de l'accident nucléaire de Three Mile Island en 1979 [Perrow, 1982]. Perrow introduit l'idée que dans les systèmes technologiques et les organisations complexes, les accidents graves sont « normaux » et donc inévitables [Perrow, 1999] et ce, indépendamment de ce qui peut être fait pour les éviter. Dans le cadre de sa théorie relativement pessimiste, Perrow définit deux dimensions : la « complexité interactive » et le « couplage fort », qui déterminent la susceptibilité d'un système aux accidents.

Un système complexe est composé de nombreux éléments interagissant entre eux de façon parfois extrêmement élaborée. Les interactions linéaires surviennent lors d'opérations de maintenance ou de production et sont relativement visibles même lorsqu'elles revêtent un caractère inattendu ; les interactions complexes ne sont, elles, pas familières ou constituent des séquences imprévues ou inattendues et ne sont ni visibles ni compréhensibles immédiatement [Perrow, 1984]. Ainsi, la complexité interactive se réfère à la présence dans un système d'une séquence d'évènements non prévue, qui s'avère soit invisible soit non immédiatement compréhensible. Si la complexité interactive peut augmenter la probabilité d'incidents dangereux, Perrow

introduit la notion de « couplage fort » pour expliquer l'origine d'un accident normal.

De manière générale, un couplage d'éléments (fort ou faible) dans un système affecte sa capacité à répondre à une perturbation pouvant mener à un accident. Un système à couplage fort est un système extrêmement interdépendant : chaque partie du système est fortement reliée aux autres ; un changement dans une partie affecte donc les autres parties. Ces systèmes peuvent être caractérisés par de très nombreuses rétroactions entre les différents éléments. Les systèmes fortement couplés répondent rapidement aux perturbations mais la réponse peut s'avérer désastreuse. Ainsi, les systèmes à couplage fort possèdent de nombreux processus interdépendants d'un point de vue temporel avec l'apparition rapide d'interactions prévues ou non. De plus, dans ce type d'organisations, les activités peuvent être considérées comme des invariants du fait des contraintes de couplage.

Selon la théorie de l'accident normal, les systèmes interactivement complexes et fortement couplés rencontrent immanquablement des accidents qu'ils ne peuvent éviter. Lorsque le système est interactivement complexe, des interactions entre défaillances indépendantes peuvent survenir, que les concepteurs n'avaient pas anticipées. Si le système est fortement couplé également, les effets s'enchaînant peuvent mener à une perte de contrôle par les opérateurs avant que ces derniers ne prennent la mesure de la situation et n'appliquent des éventuelles actions correctives. Perrow appelle ces systèmes des « accidents » [Perrow, 1999].

Contrairement à l'approche HRO qui est traitée dans le paragraphe 3.3.2, la théorie de l'accident normal est plus « structurelle » et plus « politique » :

- plus structurelle car Perrow identifie deux caractéristiques structurelles de nombreuses organisations mettant en jeu des technologies dangereuses : la « complexité interactive » et le « couplage », rendant ces organisations plus « sensibles » aux accidents ;
- plus politique car sa théorie se focalise sur l'interaction des conflits d'intérêts au sein même de ces organisations mais aussi entre ces organisations et le milieu politique. Ainsi, ces conflits d'intérêts peuvent avoir une forte influence sur la fréquence des accidents et sur leur interprétation. C'est pourquoi Perrow souligne que l'implication trop importante du politique dans les organisations sensibles sans volonté de sécurité engendre des risques inutiles [Sagan, 1993].

Perrow a fourni un travail important pour identifier la complexité interactive et le couplage fort comme des caractéristiques d'augmentation des risques au sein des systèmes ; il concluait initialement que rien ne peut être fait pour prévenir les accidents dans des systèmes complexes. Cette position très pessimiste reste fondée sur l'hypothèse que la redondance est la seule solution permettant d'améliorer la sécurité [Leveson, Dulac, Marais, Carroll, 2005]. Parallèlement, Perrow énonce que la redondance ne saurait être bénéfique puisqu'elle introduit une complexité supplémentaire et mène donc à une prise de risque supplémentaire. En fait, il propose de nombreux exemples de dispositif de sécurité redondants ou de

procédures de travail redondantes comme la cause directe d'accidents. Sagan avait déjà montré que la redondance peut réduire l'efficacité des politiques de sécurité, notamment dans le domaine nucléaire [Sagan, 1993].

Perrow postule en effet que la réduction de la complexité et du couplage va irrémédiablement à l'encontre des intérêts des décideurs, ce qui n'est pas toujours le cas [Marais, Dulac, Leveson, 2004]. Leveson montre d'une part que la redondance et l'utilisation de systèmes de protection sont parmi les approches les moins efficaces et les plus coûteuses dans la conception de la sécurité, et d'autre part que de nombreuses approches n'utilisant pas la redondance comme solution sont efficaces en conception [Leveson, 1995]. Les approches (dont la sécurité des systèmes) les plus efficaces prennent en compte l'élimination des dangers ou réduisent de façon importante leur probabilité par des moyens autres que la redondance — par exemple en remplaçant des matériaux dangereux par des matériaux sûrs, en réduisant toute complexité inutile, par découplage, en concevant par la contrôlabilité, le suivi… Dans cet état d'esprit, Perrow met en exergue la dangerosité de la redondance et les conséquences négatives de sa multiplication dans un système technologique complexe, et avance trois raisons principales :

- la multiplication des redondances, même indépendantes, engendre *de facto* une augmentation de la complexité des organisations hautement technologiques et peut donc mener à des situations « inattendues » ;
- l'augmentation des redondances rend le système plus opaque, occultant ainsi des défaillances humaines ou techniques et créant des situations de défaillance latente ;
- enfin, la redondance crée une situation de sécurité qui engendre à son tour une prise de risque supplémentaire de la part des opérateurs.

A contrario, il est bon de souligner que la complexité et le couplage insérés dans un système permettent d'atteindre un niveau de performance supérieur, à des coûts toutefois également supérieurs. Or, des systèmes conçus plus simplement et découplés peuvent la plupart du temps atteindre les mêmes objectifs. Tout l'enjeu est alors de minimiser les compromis et de déterminer l'acceptabilité du risque. Cette approche se heurte néanmoins à un double écueil : la perception du risque, qui peut considérablement varier d'un décideur à un autre, et l'absence de solution unique et simple à un problème donné.

La seconde approche du risque organisationnel a été développée au travers de la théorie dite des organisations à haute fiabilité.

3.3.2. Les organisations à haute fiabilité

L'organisation à haute fiabilité (ou *high reliability organizations*, HRO) a été définie par Roberts [Roberts, 1989 ; Roberts, 1990] comme une organisation dangereuse exigeant un très haut niveau de sécurité pendant de longues périodes. Le domaine de

recherche des HRO s'est constitué à partir d'observations faites au cours de l'étude de deux porte-avions américains, du contrôle de trafic aérien, d'une installation nucléaire et d'une équipe de sapeurs-pompiers [La Porte, 1991], qui contredisaient les hypothèses de Perrow en suggérant que des systèmes interactivement complexes et fortement couplés peuvent fonctionner pendant de longues périodes avec peu d'accidents.

La littérature consacrée aux HRO est importante et continue de s'enrichir. Néanmoins, la plupart des chercheurs du domaine des HRO s'accordent à dire que quatre caractéristiques organisationnelles permettent de limiter les accidents et d'obtenir un haut niveau de performance :

- une priorisation de la sécurité et des performances, dans le cadre d'un consensus sur les objectifs d'une organisation [La Porte, 1991] ;
- une promotion de la culture de la fiabilité au sein de l'organisation, aussi bien centralisée que décentralisée ;
- l'utilisation de l'apprentissage organisationnel permettant de maximiser l'apprentissage des accidents, des incidents (en privilégiant notamment le retour d'expérience,) ;
- enfin l'utilisation étendue de la notion de redondance [Rochlin, 1987].

La plupart des recherches récentes dans le domaine des HRO se focalisent sur l'application de ces principes à différents systèmes ou tentent de les corréler avec les caractéristiques de performance organisationnelles comme la fiabilité [Roberts, 2005].

Comme pour la théorie de l'accident normal, plusieurs caractéristiques des HRO sont sujettes à controverse, qu'il est bon de présenter brièvement ici.

Le premier groupe de réserves porte sur le concept même de HRO. Par définition, une HRO est une organisation au sein de laquelle des dizaines de millier d'évènements potentiellement catastrophiques ne provoquent pas de catastrophe. Cette définition ne peut être acceptable que dans une culture dans laquelle les catastrophes et les accidents sont tolérables, position dont la légitimité est de plus en plus violemment mise à mal. Une défaillance catastrophique peut être vue comme une éventualité pour des activités associées à de forts dangers. Ainsi, pour éviter un problème de définition, les chercheurs du domaine des HRO les définissent de façon moins précise en soulignant que les HRO constituent des systèmes à l'origine de performances libres de tout risque d'accident [La Porte, 1996].

Malgré ce souci de définition, les spécialistes de l'approche HRO relèvent que les systèmes étudiés dans ce cadre font partie des systèmes interactivement complexes et fortement couplés tels que définis par Perrow. Quelques précisions peuvent être apportées à cette affirmation. Si le système de contrôle du trafic aérien est aussi sûr que ce qu'il peut être, c'est précisément parce que la conception du système a été délibérément découplée afin d'augmenter la sécurité. Ce système a été volontairement divisé en plusieurs secteurs indépendants des phases de vol, elles-mêmes limitées et contrôlées. Un couplage faible est également assuré par le

maintien d'un fort découplage avec l'avion ; en d'autres termes, les erreurs commises par les contrôleurs peuvent être corrigées avant un éventuel impact sur la sécurité. Des dispositifs d'alerte permettent de prévenir les accidents, comme les systèmes d'évitement de collision.

Les chercheurs HRO soulignent le faible niveau de complexité des systèmes qu'ils peuvent étudier. Comme le souligne La Porte, « les HRO prennent des décisions dans un contexte où presque tout est connu concernant les aspects techniques d'un système notamment en ce qui concerne l'identification des dangers. Les personnes dans ces organisations connaissent pratiquement tout d'un point de vue technique et sur ce qu'ils doivent faire… cette conduite engendre des processus stables qui sont assez bien compris dans chaque HRO » [La Porte, 1991]. Le fait même que ces systèmes requièrent une importante connaissance des processus va à l'encontre de la définition de la complexité interactive pour laquelle Perrow définit comme système une conception dont les interactions entre les éléments ne peuvent être planifiées, comprises ou prédites.

Le deuxième groupe de limites inhérentes à l'approche HRO porte, en dehors des systèmes dans lesquels ils sont étudiés, sur le respect de certaines pratiques. Tout d'abord, les HRO prônent l'inscription de la sécurité et de la performance au nombre des objectifs de l'organisation [Leveson, Dulac, Marais, Carroll, 2005]. En temps de paix, dans le cas des porte-avions, le but premier d'un avion est ainsi de décoller et d'atterrir de façon sûre. En cas d'accident, le pilote peut s'éjecter de façon sûre de l'appareil. Si les conditions sont risquées, par exemple en cas de mauvais temps, les opérations de vol peuvent être retardées ou annulées avec d'importantes conséquences — ce qu'il ne sera pas possible de faire en cas de guerre…Ainsi, dans un contexte différent, il peut s'avérer difficile d'attacher le même degré de priorité à la sécurité qu'à la performance.

Par ailleurs, les HRO prônent la promotion d'une culture de fiabilité lors d'opérations centralisées et décentralisées. Cette caractéristique des HRO socialise les membres de l'organisation et les entraînent à fournir des réponses uniformes et appropriés aux situations de crise [Weick, 1987]. Ce niveau de réponse à une crise est une réponse décentralisée qui forme une importante partie de la philosophie HRO. D'un autre côté, une centralisation simultanée se réfère au maintien de la chaîne de commandement en cas de crise. La Porte suggère que, lors des opérations d'un porte-avions américain soumis à la chaîne de commandement de la Marine, un simple matelot puisse annuler un atterrissage [La Porte, 1991] ; il prendrait en effet trop de temps de respecter la chaîne de commandement jusqu'à son sommet. Notons également que les personnels de niveau les plus bas ne peuvent prendre des décisions que dans un seul sens, notamment lorsque les délais de décision sont extrêmement courts. Toutefois, les situations n'exigeant pas de délai de décision bref présentent aussi un intérêt méthodologique ; La Porte souligne que l'ensemble des personnels sont entraînés à reconnaître un problème quand ils le voient jusqu'à ce qu'il soit résolu ou jusqu'à ce qu'une personne pouvant le résoudre décide de

prendre la responsabilité de le faire [La Porte, 1991]. Cette approche a montré son efficacité lorsque les systèmes étudiés sont faiblement couplés ; dans les systèmes interactivement complexes et fortement couplés, toute action individuelle peut mener à des accidents lorsque les décisions locales ne sont pas coordonnées avec les décisions globales.

L'utilisation de l'apprentissage organisationnel permet d'optimiser l'apprentissage relevant des accidents. En effet, les HRO exploitent « l'imagination, les histoires, les simulations et autres représentations technologiques » afin de pouvoir apprendre des erreurs [Weick, 1987]. Les ingénieurs mettent en œuvre un tel processus lorsqu'ils cherchent à analyser les dangers. Il est difficile d'argumenter contre un apprentissage des erreurs et des accidents mais dans les systèmes complexes, où les erreurs peuvent avoir des conséquences disproportionnées, les difficultés d'apprentissage ne doivent pas être sous-estimées. De nombreux obstacles ont été identifiés, qui limitent l'efficacité de l'apprentissage à un petit nombre de problèmes. March fournit une étude des bénéfices et des limites de l'apprentissage de l'expérience [March, 1991]. L'apprentissage se trouve ainsi limité par les interprétations des causes des accidents et des incidents, elles-mêmes sous l'emprise d'influences économiques, légales ou politiques. Leplat a montré que les individus identifient de façon différente les causes des accidents en fonction de leur statut ou de leur position dans une organisation [Leplat, 1987].

Par ailleurs, l'apprentissage organisationnel des incidents présente des coûts très élevés. L'apprentissage à partir des erreurs ne représente pas un moyen d'apprentissage efficace, particulièrement dans les systèmes complexes, dans lesquels les facteurs impliqués dans les accidents peuvent être très nombreux. En résumé, apprendre des accidents n'est ni le seul ni le meilleur moyen pour réduire les accidents dans les systèmes techniques.

Les organisations étudiées dans le cadre des HRO sont caractérisées par des changements lents en conception afin d'apprendre à partir des accidents. Les retours d'expérience d'organisations recourant à des technologies plus anciennes, voire dépassées, sont souvent inexploitables pour des organisations plus récentes.

Enfin, la dernière réserve émise à l'encontre de la démarche HRO porte sur l'utilisation presque systématique de la redondance afin d'accroître la sûreté et la performance du système. La redondance vise avant tout à augmenter le niveau de sécurité dans les systèmes socio-techniques, mais cette position demeure un point de désaccord entre les HRO et la théorie de l'accident normal. Répétons-le, chaque théorie est conçue pour des systèmes précis. La complexité interactive, le couplage fort et le travail dans un environnement incertain limitent l'efficacité de la redondance, qui peut alors, et paradoxalement, augmenter les risques d'accident [Perrow, 1999 ; Sagan, 2004].

Dans les systèmes HRO, la redondance peut contribuer à la prévention des défaillances d'éléments simples — mais *sous certaines conditions*. La redondance est liée à l'hypothèse de la défaillance « aléatoire » d'un élément du système ayant des

conséquences sur son efficacité. Or, dans des systèmes interactivement complexes et fortement couplés, de nombreuses causes d'accidents ne procèdent pas d'une défaillance de composant aléatoire. En effet, les systèmes complexes sont pour l'essentiel protégés dès leur conception des accidents par défaillance d'éléments, c'est-à-dire en évitant que l'accident ne soit causé par des dysfonctionnements dans les interactions entre les éléments. Le même raisonnement s'applique aux éléments humains et aux processus de décision.

La redondance s'avère efficace lorsque la démarche de sécurité est exclusivement fondée sur elle et que nul autre besoin de mesures de sécurité supplémentaires ne s'est fait jour. Par exemple l'accident de la navette *Challenger* est en partie dû à une confiance trop importante en la redondance, notamment sur le joint responsable de l'accident. La défaillance du premier joint a mené à la défaillance du second joint [Leveson, 1995]. Les redondances ne protègent donc pas des erreurs de conception, mais uniquement des défaillances d'élément.

Dans le cas de systèmes contenant des logiciels, les redondances s'avèrent inutiles pour protéger les systèmes contre des commandes pouvant mener à des accidents. En effet, la plupart des accidents dus à des logiciels peuvent être considérés comme étant dus à des erreurs de programmation, c'est-à-dire à une incompréhension dans ce que le logiciel est supposé faire sous certaines conditions. Dans ce type d'accident, le logiciel n'est pas défaillant au sens où un élément matériel pourrait l'être : à moins d'une erreur de programmation, un logiciel exécute exactement ce que le programmeur a codé, ce qui est différent d'une défaillance matérielle, où le système rencontre une situation inattendue. De plus, les systèmes de management de la redondance sont si complexes qu'ils induisent fréquemment des erreurs pouvant mener à des défaillances matérielles. La redondance ne constitue donc qu'un moyen limité d'amélioration de la fiabilité (mais pas nécessairement de la sécurité) — encore faut-il préciser qu'elle n'est efficace que dans certains cas car elle peut, dans d'autres conditions, être la source d'accidents.

En résumé, les HRO ne tiennent pas assez compte de l'incertitude au sein des systèmes complexes ; si elle perçoit cette difficulté, la théorie de l'accident normal sous-estime quant à elle les différents moyens de faire face à cette incertitude. Les deux approches font de la redondance le seul moyen de considérer le risque. La contribution de Perrow à la compréhension des accidents dans les systèmes complexes ne se limite pas à l'identification d'une « complexité interactive » et d'un « couplage fort » comme des facteurs critiques ; sa vision *top-down* des accidents, comme la vision *bottom-up* (qui correspond à la fiabilité des composants) des HRO, sont préjudiciables à la compréhension même des accidents. Cette théorie incomplète mène à un pessimiste plus important que nécessaire dans le cadre de la conception de systèmes à hauts risques. Quant aux HRO, la plupart de leurs propositions se révèlent extrêmement coûteuses, voire inapplicables dans les systèmes socio-techniques ; dans d'autres cas, ces propositions ont tendance à trop simplifier les problèmes et sont donc inefficaces. Enfin, ces deux approches ont une vision non

dynamique de l'état d'un système ; or, les systèmes complexes évoluent dans le temps si bien que seule une vision dynamique permet de mieux les comprendre et de les analyser. Ce constat est l'objet du chapitre suivant, qui présente les modèles d'accident systémiques.

Résumé des théories organisationnelles

Pour Sagan, les HRO et la théorie de l'accident normal présentent des hypothèses tout à fait plausibles et logiques [Sagan, 1993].

Néanmoins, elles sont toutes les deux basées sur une approche empirique. Il importe dès lors de se demander si l'une ou l'autre peut estimer précisément la probabilité d'occurrence d'un accident grave dans une organisation hautement technologique.

Le tableau 2 présente les principales caractéristiques des deux approches.

Théorie HRO	Théorie de l'accident normal
Les accidents peuvent être évités par le biais d'une bonne gestion et d'une bonne conception organisationnelle.	Les accidents sont inévitables dans les systèmes complexes et fortement couplés.
La sécurité est la priorité organisationnelle.	La sécurité est un des nombreux objectifs de l'organisation.
Les redondances améliorent la sécurité.	Les redondances sont souvent à l'origine des accidents.
Des processus de réponse décentralisés sont nécessaires pour permettre des réponses adaptés aux surprises.	Contradiction organisationnelle : une décentralisation est nécessaire pour la complexité mais une centralisation est indispensable pour les systèmes fortement couplés.
Une culture de la fiabilité améliorera la sécurité en encourageant des réponses adéquates et uniformes.	Un modèle militaire de discipline, de socialisation et d'isolement est incompatible avec des valeurs démocratiques.
La continuité des opérations, l'entraînement et la simulation permettent de maintenir des opérations hautement fiables.	Les organisations ne peuvent pas s'entraîner dans le cadre d'opérations incertaines.
Les procès et les erreurs des accidents peuvent être efficaces et peuvent être complétés par des simulations ou des mesures d'anticipation.	La non-prise de responsabilité face à l'accident paralyse les efforts d'apprentissage organisationnel.

Tableau 2 ■ Caractéristiques des HRO et de l'accident normal
adapté de Sagan, 1993

Conclusion

La compréhension de l'accident passe par une démarche qui vise à le définir dans un contexte afin de mieux l'appréhender. Ce chapitre a donc dans un premier temps présenté ce qu'est un accident à partir de différentes définitions permettant de mettre en évidence l'évolution de cette notion au travers de divers disciplines et époques. Cette définition permet donc de le comprendre mais également de le « domestiquer » afin de ne plus le considérer comme la simple « main de Dieu » ou une fatalité. Cette première étape a été suivie par une démarche de représentation. En effet, comprendre un accident c'est aussi être capable de se le représenter, notamment par le biais d'un modèle. Les modèles d'accident sont devenus des outils indispensables à la représentation d'un évènement accidentel. Au cours du XX^{e} siècle, ces modèles ont revêtu diverses formes : d'abord « séquentiels », fondés sur une approche analytique et linéaire (l'exemple le plus significatif étant le modèle d'Heinrich), ils ont ensuite été organisationnels mais linéaires dans le cas du modèle de Reason ou

dans celui des théories organisationnelles du risque (théorie de l'accident normal de Perrow ou HRO du groupe de Berkeley).

Ces différents modèles montrent aujourd'hui leurs limites dans des systèmes complexes où les progrès technologiques et les pressions modifient le cœur même des organisations. Il semble donc aujourd'hui nécessaire de changer de paradigme en écartant toute approche linéaire et en complétant l'approche analytique par une approche systémique et dynamique. Les modèles d'accident dits « systémiques » semblent mieux répondre aux contraintes des systèmes socio-techniques et hautement technologiques dont les migrations vers des états dangereux ou accidentels sont considérées comme non linéaires. Cette approche systémique de l'accident fait l'objet du chapitre suivant.

Chapitre 2
L'accident comme un système

Les systèmes hautement technologiques considérés comme des systèmes socio-techniques peuvent être l'objet d'un accident, voire d'une catastrophe.

De nombreux accidents tels que le rejet de gaz toxiques et mortels lors de la catastrophe de Bhopal [Srivastava, 1992], l'accident d'hélicoptères américains BlackHawk lors de la guerre du Golfe en 1994 [AAIB, 1994], l'explosion de la navette de la NASA *Challenger* [Vaughn, 1996], l'accident de train de Varsovie en 1996 [Höhl et Ladkin, 1997] ou l'accident de l'installation d'Esso à Longford [Hopkins, 2000] sont des exemples de défaillances systémiques dans des systèmes complexes ayant mené à des pertes humaines et matérielles.

Ces accidents systémiques s'expliquent en partie par un couplage fort parmi leurs éléments et par de fortes contraintes organisationnelles [Woods *et al*., 1994]. Dans ces systèmes, les accidents se développent pendant un certain temps et apparaissent comme le résultat de défaillances au niveau matériel et humain [Perrow 1984 ; Reason, 1990].

Comprendre les causes des accidents dans les systèmes complexes permet d'en garantir le niveau de sécurité et de développer des stratégies de prévention d'accidents similaires futurs. Ce chapitre a donc pour ambition de présenter la vision systémique de l'accident, notamment celle adoptée dans l'analyse des accidents dans les systèmes socio-techniques. Ainsi, une première section présente brièvement ce que sont un système et un système complexe, tandis qu'une deuxième section considère l'accident comme un système. Dans un troisième et dernier temps, les modèles d'accidents systémiques sont présentés afin de comprendre et de gérer les accidents au sein des systèmes complexes.

1. La systémique

La vision systémique de l'accident est une tentative de réponse aux limites des approches analytique et linéaire. La méthode analytique a longtemps prévalu en Occident, faisant de ce réductionnisme un quasi-dogme scientifique [Le Moigne,

1977], basé sur une conception scientifique selon laquelle « il serait impossible de parvenir à comprendre les systèmes complexes si l'on n'avait pas commencé au préalable par isoler les diverses parties qui les composent » [Commoner, 1972].

L'une des caractéristiques de la méthode scientifique et analytique est sa prétention à l'universalité, vocation contrariée par plusieurs limites :

- l'isolement artificiel des disciplines les unes par rapport aux autres ;
- le réductionnisme de la définition des problèmes ;
- la faible capacité de résolution des problèmes complexes ;
- la propension à n'envisager qu'une seule chose à la fois et à en déduire des généralités.

Ces velléités se sont renforcées lorsqu'a émergé le besoin de comprendre des systèmes de plus en plus complexes — à forte intensité technologique notamment, comme l'aviation, le transport maritime, le contrôle du trafic aérien, les installations nucléaires, les industries de la défense ou l'aérospatial, ou encore dans des secteurs comme la chimie, la pétrochimie ou la santé. Dépassés, les modèles d'accident traditionnels s'avèrent inadaptés à l'analyse des accidents survenant dans les systèmes socio-techniques modernes, dans lesquels l'accident ne résulte pas d'une unique défaillance technique ou humaine. La recherche de méthodologies susceptibles de composer avec cette complexité a donc vu le jour dans de nombreuses disciplines, et notamment dans le domaine de l'accident. L'une de ces méthodologies connaît une expansion rapide, dont la notion de système est au cœur.

1.1. Le système

Le concept de système s'est principalement développé à partir des années 1940 dans différents domaines des sciences et techniques tels que la biologie, l'économie, voire le domaine militaire. De grands auteurs sont aujourd'hui considérés comme des précurseurs de la pensée système :

- Norbert Wiener professeur au MIT, auteur de l'ouvrage *Cybernetics* (1948), qui posa les fondements de la cybernétique, considérée comme la science des systèmes et contribua fortement au développement de la théorie du contrôle ;
- Ludwig von Bertalanffy et sa théorie générale des systèmes (parfois désignée sous les vocables de « théorie générale du système » ou « théorie du système générale »), publiée en 1968 ;
- Jay Forrester, qui élargit le champ d'application de la nouvelle théorie des systèmes à la dynamique des systèmes, élaborant par la suite une dynamique générale des systèmes à partir des années 1950.

Forrester définit un système comme un « groupe de parties opérant ensemble pour un objectif commun » [Forrester, 1972]. Un système est donc un groupe d'éléments interreliés, interagissants ou interdépendants formant un ensemble complexe unifié. Hall précise qu'un système ou que l'ingénierie système « ne peut

probablement pas être résumée à une définition claire et tranchée ». Il y a cependant plusieurs définitions fondées sur la littérature et Hall apporte la sienne : « un système est une configuration d'objets possédant des relations entre les objets et leurs attributs » [Hall, 1962]. Dommasch définit un système complet comme « n'importe quel équipement complexe, existence humaine ou interrelation conçus pour effectuer une tâche donnée quoi qu'en soit la manière. Logiquement, les grands systèmes sont divisés en sous-systèmes pour être en harmonie comme des blocs formant un système global » [Dommasch, 1962].

Dans son ouvrage de 1991, Rechtin définit un système comme « un ensemble de choses travaillant ensemble afin de produire quelque chose de plus grand… un système possède des propriétés propres qui sont illimitées — chaque système est une part inhérente d'un système encore plus grand » [Rechtin, 1991]. Il ajoute :

- « Un système est une organisation complexe d'éléments ou parties différents connectés et reliés pour former un ensemble organique ;
- l'ensemble est plus grand que la somme des parties, ce qui signifie que le système possède des propriétés plus importantes que ses parties. En fait, l'objectif d'un système est de posséder ces nouvelles propriétés ».

Les composants d'un système peuvent être des objets physiques tangibles ; les composants peuvent aussi être impalpables tels que des processus, des relations, des règlements intérieurs, des flux d'informations, des interactions interpersonnelles ou des états internes tels que des sentiments, des valeurs ou bien des croyances.

Les systèmes possèdent 5 caractéristiques essentielles permettant de les cerner [Gharajedaghi, 2006].

■ **L'interaction :** elle porte sur la causalité dans un système [Durant, 1979][Garbolino, 2010]. Les parties d'un système doivent toutes être présentes afin que le système remplisse son objectif de façon optimale. Séparer les éléments d'un système sans toucher à ses fonctions ou à ses relations revient à constituer une collection d'éléments et non un système ; de la même façon, ajouter des éléments à une collection sans modifier ses fonctions et ses relations revient à bâtir une nouvelle collection. À l'inverse, assigner de nouvelles tâches à un groupe conduit à modifier les fonctions et les relations de ce groupe, conduisant à la création d'un système. Un système remplit donc une certaine fonction pouvant être définie comme le but identifiable par un observateur.

■ **La structure :** les parties d'un système doivent être organisées d'une certaine façon pour que le système puisse atteindre son objectif. Placés dans un ordre aléatoire, les éléments d'une collection ne peuvent constituer un système. Un système est composé d'une constellation d'éléments et d'une structure qui détermine sa fonction, son but, son comportement et son identité. Ainsi un système est indivisible et son but même ne peut être atteint dans son intégralité si un ou plusieurs éléments sont supprimés.

■ **L'émergence :** chaque système a un but particulier en relation avec un système plus important au sein duquel il est inclus. Un système possédant son propre objectif et étant une entité discrète ayant une certaine intégrité maintenant ensemble ses constituants, il est impossible d'unir un ou plusieurs systèmes pour en obtenir un nouveau plus important.

Selon le même raisonnement, il n'est pas possible de diviser un système pour obtenir des systèmes plus petits fonctionnant à l'identique.

■ **L'auto-organisation :** tout système maintient son équilibre grâce à des fluctuations et des ajustements. Laissé à lui-même, le système cherche à maintenir son équilibre. Un système atteint sa stabilité à travers des fluctuations, des interactions, des rétroactions et des ajustements qui circulent de façon continue au sein de ses différentes parties ainsi qu'entre le système et son environnement.

■ **La rétroaction :** tout système possède des boucles de rétroaction. La rétroaction désigne la transmission et le retour d'informations. La caractéristique la plus importante de la rétroaction est qu'elle constitue le catalyseur d'un changement de comportement en initiant un processus d'auto-organisation. Un système possède ses propres rétroactions ; mais constituant lui-même une partie d'un système plus important, il possède aussi des rétroactions avec les systèmes extérieurs.

Dans certains systèmes, les processus de rétroaction et d'ajustement se mettent en place si rapidement qu'il est relativement facile pour un observateur de les suivre. Dans d'autres, la rétroaction peut se révéler beaucoup plus lente, de sorte qu'un observateur peut éprouver des difficultés à identifier l'action incitant la rétroaction. Finalement, la rétroaction n'est pas nécessairement transmise et effectuée à travers le même élément du système ou à travers le même système. Elle peut s'effectuer par le biais de plusieurs éléments intervenant dans un premier système et retournant dans un système extérieur avant de finalement parvenir à l'élément du système initial.

D'une façon générale, l'étude des systèmes passe par l'intégration de principes résumés dans le tableau 3.

L'approche systémique
■ Relie : se concentre sur les interactions entre les éléments
■ Considère les effets des interactions
■ S'appuie sur la perception globale
■ Modifie des groupes de variables
■ Intègre la durée et l'irréversibilité
■ Valide les faits par comparaison du fonctionnement du modèle avec la réalité
■ Recourt à des modèles insuffisamment rigoureux pour servir de base aux connaissances, mais utilisables dans la décision et l'action
■ Est efficace lorsque les interactions sont non linéaires et fortes
■ Conduit à un enseignement pluridisciplinaire
■ Conduit à une action par objectifs
■ Apporte une connaissance des buts, mais les détails demeurent flous

Tableau 3 ■ L'approche systémique
adapté de De Rosnay, 1975

1.2. Le système complexe

Au-delà des caractéristiques fondamentales des systèmes existent des systèmes complexes dotés d'un comportement différent et posant des défis nouveaux aux systémiciens. En action, un système complexe possède de nombreuses variables, divers facteurs entrant en jeu et plusieurs éléments semi-indépendants et interreliés. La représentation d'un système complexe montre des boucles de rétroaction en évolution, tandis que la durée et la longueur des retards sont elles aussi susceptibles de variations ; un certain nombre de structures peuvent sembler en conflit.

La notion de complexité est une source importante d'incertitude, en rendant difficiles la compréhension et la prévision du comportement d'un système. Si plusieurs raisons peuvent expliquer la complexification d'un système, la complexité apparaît comme la réponse permettant de satisfaire de nombreuses exigences — par exemple, les exigences de performance. Bien que certaines approches de conception de systèmes diminuent la complexité au lieu de conserver la fonctionnalité [Leveson, 1995], un niveau minimum de complexité, ou une complexité essentielle, demeurent requis, qui croît en essayant de satisfaire les exigences du système.

La complexité augmente également avec la taille de tout système non linéaire.

Les systèmes complexes possèdent 5 caractéristiques principales [Gharajedaghi, 2006] :

- **Les systèmes complexes ont tendance à s'autostabiliser :** la représentation en boucles causales d'un système complexe contient probablement un grand nombre de boucles stabilisatrices, chacune agissant sur un élément plus petit du système en équilibre ou fonctionnant à proximité du niveau désiré. Cette caractéristique suggère que beaucoup d'organisations complexes résistent aux changements ou aux campagnes d'amélioration et retrouvent éventuellement leur état initial : toutes les boucles stabilisatrices sont conçues pour maintenir un système dans un état originellement déterminé.
- **Tous les systèmes complexes ont un objectif :** un système complexe contient de nombreuses boucles stabilisatrices (ou boucles négatives), chacune d'elles visant à maintenir un niveau de performance désiré ou un but. Un système complexe peut contenir de nombreuses boucles explosives (ou boucles positives) servant à accroître ou à diminuer certains phénomènes au sein du système. Dans un système complexe tel qu'une organisation, les buts peuvent par exemple s'exprimer en termes de croissance ou de stabilisation, tout en étant explicites et connus des membres de l'organisation. Néanmoins, ces processus peuvent être contradictoires, ambigus ou implicites, et le système est tributaire de la subjectivité de chacun.
- **Tout système complexe est capable d'utiliser des boucles de rétroaction afin de modifier son comportement :** cette capacité crée des opportunités de changement et d'évolution au sein du système, surtout si la rétroaction est explicite et accessible. Par exemple, le potentiel d'amélioration d'une organisation est d'autant plus élevé qu'elle cherche à rassembler les informations concernant les problèmes tels que des délais d'envoi ou la complexité de ses procédures. Pour tout système étudié, une bonne compréhension de la structure et des fonctionnements du système rend plus facile la mise en œuvre de cette importante capacité afin de catalyser les changements internes au système.
- **Un système complexe peut modifier son environnement :** un système cherchant à atteindre son objectif et se montrant capable de modifier son propre comportement, il n'est pas surprenant qu'il puisse ainsi modifier son environnement pour atteindre ses objectifs. L'identification des liens entre le système et son environnement revêt alors une importance cruciale. Chaque système constituant un élément d'un système plus grand, il est possible d'anticiper dans quelle mesure et selon quelles modalités les changements introduits dans un système peuvent mener à des changements dans son environnement.
- **Un système complexe est capable de se répliquer, se maintenir, se réparer et se réorganiser par lui-même :** puisque les systèmes changent en réponse à leur environnement, même des organisations semblant parfaitement identiques possèdent probablement des excentricités ou des divergences. De plus, une organisation altérée de façon brutale trouve très souvent des voies afin de

recouvrer ses fonctions essentielles ou de se réorganiser par elle-même pour poursuivre ses objectifs premiers.

Ces particularités mettent en exergue d'importantes capacités d'évolution et de fonctionnement de la part des systèmes complexes. Ces singularités ne sauraient toutefois occulter leurs 4 faiblesses principales [Gharajedaghi, 2006] :

- des objectifs conflictuels ;
- le dilemme centralisation / décentralisation ;
- des rétroactions biaisées ;
- la perte d'anticipation.

Dans un système complexe, il n'est pas rare qu'un sous-système poursuive des objectifs entrant directement en compétition avec les objectifs du système global. Les contraintes imposées par cette compétition à l'intérieur même du système, voire au niveau des rétroactions, n'est pas sans conséquences. Ainsi, les boucles de rétroaction rassemblées à partir des sous-systèmes pour l'utilisation dans un système plus large peuvent être soit imprécisément transmises, soit imprécisément interprétées. Ce problème de « communication » peut notamment se faire ressentir dans le domaine de la sécurité avec des impacts plus ou moins néfastes sur la performance d'un système.

C'est à partir de ces caractéristiques essentielles des systèmes que la pensée système s'est développée.

1.3. La pensée système

La pensée « système » a introduit des outils, mais aussi un véritable cadre de travail pour l'analyse des problèmes dans des ensembles complexes ; elle structure désormais la pensée et la réflexion de nombreux professionnels, et constitue un langage permettant de communiquer sur des complexités dynamiques et d'interdépendances entre éléments ou entités.

La pensée système repose sur deux principales dyades conceptuelles : le bipôle émergence / hiérarchie d'une part, le bipôle communication / contrôle d'autre part [Checkland, 1999].

C'est le concept de complexité organisée qui permet d'expliciter la notion de hiérarchie des niveaux d'organisation, chacun étant plus complexe que le niveau inférieur ; chaque niveau est caractérisé par des propriétés émergentes n'existant pas à un niveau inférieur. La théorie de la hiérarchie est fondée sur la différence fondamentale entre un niveau de complexité et un autre ; son objectif est de fournir une description des interactions entre les différents niveaux et de comprendre la formation des hiérarchies. Cette théorie est construite sur la propriété suivante : des propriétés émergentes, associées à un ensemble d'éléments à un certain niveau hiérarchique, sont liées à un certain nombre de contraintes sur les degrés de liberté du système ; les propriétés émergentes résultent de l'application de contraintes et

c'est cette imposition de contraintes sur l'activité d'un niveau qui permet de définir les lois d'interaction d'un niveau. Les hiérarchies sont caractérisées par des processus de contrôle à l'interface entre les niveaux [Checkland, 1999].

Cette notion de contrôle amène directement à la seconde dyade conceptuelle, polarisée autour de la communication et du contrôle. Cette hiérarchie systémique entraîne une communication entre les niveaux facilitant l'adaptation à l'environnement. Cette dyade de concepts s'est traduite notamment par le développement de la « cybernétique » par Norbert Wiener qui la définit comme « la théorie de la communication et du contrôle au sein des machines et des animaux » [Wiener, 1948]. Ces travaux sont notamment à la source du concept de « rétroaction ».

Les notions de hiérarchie et de contrôle ont permis de définir le principe de contrôle hiérarchique. En général, un contrôle hiérarchique requiert la satisfaction de trois conditions [Checkland, 1999] :

- l'imposition d'une contrainte doit entraîner de nouvelles relations fonctionnelles (avec le niveau inférieur) ;
- l'imposition d'une contrainte doit être optimale, c'est-à-dire qu'elle ne doit être ni trop rigide ni trop souple ;
- enfin, l'imposition d'une contrainte doit pouvoir influer sur la dynamique du niveau inférieur.

Le développement de l'approche systémique a provoqué l'émergence de quatre grandes caractéristiques de la pensée système (figure 4) :

- une pensée holistique (des points de vue structurel, fonctionnel et processuel) ;
- une pensée opérationnelle (une dynamique des systèmes aux boucles de rétroaction multiples, applicable dans des situations de chaos et de complexité) ;
- une auto-organisation, avec une évolution vers un ordre prédéfini (modèle socio-culturel ou socio-technique) ;
- une conception interactive (reconception du futur).

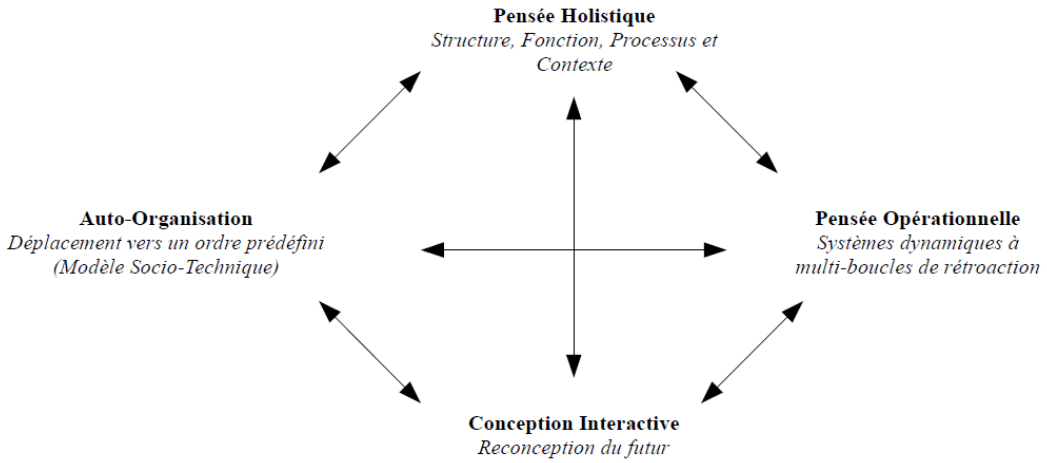


Figure 4 ■ Caractéristiques systémiques
adapté de Gharajedaghi, 2006

La pensée système se singularise avant tout par sa focalisation sur le « tout ». Une croyance répandue fait de l'approche multidisciplinaire une approche système — ce qu'elle n'est pas : la capacité à synthétiser des résultats dans un ensemble cohérent et en interaction est de loin plus cruciale que la capacité à générer de l'information à partir de perspectives et de disciplines différentes.

Malgré leur succès, trois approches prenant en compte les systèmes (pensée analytique, pensée synthétique et science du comportement) peinent encore à s'accorder avec la méthode holistique :

- l'analyse a constitué l'essence de la pensée scientifique classique. La méthode scientifique admet que l'ensemble se résume à la somme des parties, de sorte que la compréhension de la structure constituerait une condition nécessaire et suffisante à l'appréhension de l'ensemble ;
- la synthèse a été le principal instrument de l'approche fonctionnelle. En définissant un système en fonction de son état final, la synthèse place le sujet dans un contexte plus large que le système auquel il appartient, et étudie les effets qu'il peut produire sur son environnement ;
- l'approche processuelle s'est longtemps focalisée sur la science comportementale, cherchant à formuler une réponse nécessaire pour la définition d'un tout ;

Ainsi, l'approche holistique des systèmes fournit une vision globale d'un ensemble, tout en s'intéressant aux éléments ; elle s'efforce de caractériser les processus, la structure, la fonction et le contexte.

1.4. Processus, structure, fonction et contexte

Cependant, comprendre un « ensemble » exige de comprendre une structure, une fonction et un processus à un moment donné [Gharajedaghi, 2006]. Ces trois notions représentent les trois éléments qui, associés dans un environnement donné, forment un tout.

La structure, la fonction et le processus et le contexte permettent de définir et de comprendre un « ensemble » :

- la structure définit les éléments et leurs relations ;
- la fonction représente les résultats ou les effets produits ;
- le processus définit de façon explicite la séquence des activités et la façon dont les résultats sont produits ;
- enfin, le contexte définit l'environnement unique dans lequel le système est situé.

Ainsi, il est communément admis que pour comprendre un système, il est nécessaire de comprendre sa structure, d'où la prédominance de l'étude de la structure dans la science classique. Selon Ackoff, une structure donnée peut produire

plusieurs fonctions dans le même environnement [Ackoff, 1971]. Par exemple, la structure d'une entreprise, créatrice de richesse, peut produire des fonctions sécurité dans une démarche globale d'amélioration de la performance. Des structures différentes peuvent également produire une fonction donnée — par exemple, la fonction de transport peut être remplie par différents moyens tels que le train, l'avion ou la voiture (figure 5).

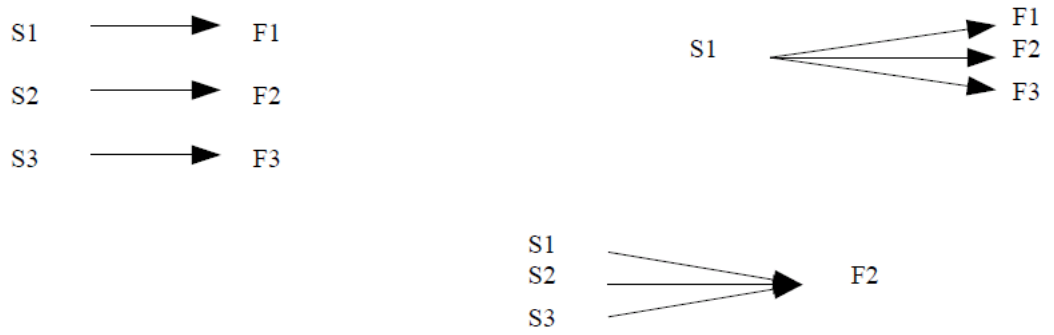


Figure 5 ■ Liens entre la structure et la fonction
adapté de Gharajedaghi, 2006

La notion classique de causalité, où la cause est la condition nécessaire et suffisante à l'apparition de son effet, prouve son inadéquation à expliquer ce phénomène. En effet, la production de différentes fonctions par une simple structure dans le même environnement peut être expliquée par la coexistence de différents processus dans la même structure, qui produisent différentes fonctions.

Cependant, lorsque plusieurs fonctions existent pour une structure donnée dans un environnement donné et lorsque les processus au sein de cette structure deviennent connus, alors structure et fonctions permettent la compréhension de l'ensemble. Structure, fonction et processus au sein d'un environnement et d'un contexte donnés forment un ensemble interdépendant de variables collectives et exclusives.

Réunies, ces quatre notions définissent l'ensemble ou rendent du moins possible sa compréhension, donc celle du comportement du système.

La présence simultanée de variables interdépendantes conduit à une relation circulaire, où chaque variable coproduit les autres et est coproduite par les autres. Affirmer que ces variables forment la base demeurerait toutefois imprécis dans la mesure où chacune d'elles ne peut exister sans la présence des autres ; elles doivent évoluer au même moment. Une erreur fréquente consiste à ne pas considérer le système dans son ensemble. L'approche holistique demande au contraire d'appréhender chaque variable dans sa relation avec les autres, dans une configuration donnée. Par conséquent, dans une vision systémique, ces caractéristiques essentielles contribuent à comprendre l'accident.

2. La systémique de l'accident et de l'état accidentel

Dans une vision holistique d'un système, il est donc possible de définir « 3 + 1 » caractéristiques visant à définir le système. Ces « 3 + 1 » caractéristiques ont par ailleurs la capacité à décrire un accident systémique.

Un système complexe est avant tout un système dynamique dont le comportement change au cours du temps, au niveau des éléments ou de leurs interactions. Ce comportement est le résultat de contrôles au sein du système, susceptibles d'engendrer de nouvelles configurations et de nouvelles caractéristiques, voire d'une dynamique pouvant mener le système vers un état dangereux, allant parfois jusqu'à un « état accidentel ». En effet, l'évolution des caractéristiques d'un système affecte aussi bien la fonction, la structure que les processus. Or, ces trois dimensions ont, dans un contexte donné, la capacité de définir un comportement et donc un état. Pour un système, il est donc possible de définir un « état accidentel » d'un système comme « le résultat de la migration de ses caractéristiques systémiques dans un contexte donné se traduisant par des dommages ou des pertes ». L'état accidentel se traduit par une dégradation des processus, de la structure et de la fonction. Cette migration peut être lente ou immédiate et débuter à n'importe quel niveau d'un système ou d'une organisation complexe. La sécurité constitue donc un phénomène émergent dans un système dynamique et il est difficilement concevable de comprendre un accident sans comprendre le système lui-même et ses fondements. L'objet du paragraphe suivant est de présenter la notion de sécurité au regard de la théorie des systèmes.

2.1. Théorie des systèmes et sécurité

La théorie des systèmes, qui date des années 1930-1940, est une réponse aux techniques d'analyses classiques face à l'accroissement des systèmes complexes. Norbert Wiener [Wiener, 1986] appliquait cette approche dans le domaine de l'ingénierie du contrôle et des communications alors que Ludwig von Bertalanffy [von Bertalanffy, 1968] la développait dans le domaine de la biologie.

Les méthodes scientifiques traditionnelles divisent les systèmes en sous-systèmes distincts pouvant être analysés séparément ; les aspects physiques des systèmes sont décomposés en éléments physiques et le comportement est séparé en évènements au cours du temps [Leveson, 2006]. Une telle décomposition suggère que chaque sous-système fonctionne de façon indépendante et que les résultats d'analyse ne sont pas contradictoires lorsque les éléments sont analysés séparément. Dans ce cadre, les éléments et les évènements ne font l'objet d'aucune rétroaction ni interaction non linéaire, et leur comportement est le même qu'ils soient analysés individuellement ou bien groupés. Cette description s'opère dans le cadre d'une « simplicité organisationnelle » [Weinberg, 1975]. De tels systèmes peuvent être séparés en sous-systèmes non interactifs pour les besoins de l'analyse car la nature précise de

l'interaction des éléments est connue et ces interactions peuvent être examinées par paires.

Un autre type de systèmes apparaît sous l'appellation de « complexité non organisée » [Weinberg, 1975], dont la structure sous-jacente manquante autorise un réductionnisme, dans un souci d'efficacité. Ces systèmes complexes ont un comportement suffisamment régulier et aléatoire pour qu'il apparaisse possible de les étudier sous l'angle statistique, la loi des grands nombres constituant l'approche usuelle.

Enfin, un troisième type de systèmes a fait émerger la notion de « complexité organisée » [Weinberg, 1975]. Ces systèmes, trop complexes pour une analyse complète, sont aussi trop organisés pour autoriser une approche statistique. La complexité organisée se focalise sur le système pris comme un ensemble et non comme des parties séparées ; elle considère que les propriétés du système ne peuvent être traitées de façon appropriée dans leur ensemble qu'en tenant compte de leurs aspects sociaux aussi bien que techniques. C'est pourquoi l'analyse des accidents passe par une approche intégrant les aspects d'une part hiérarchiques et d'autre part dynamiques du système.

2.1.1. La composante hiérarchique

Le concept de hiérarchie de niveaux d'organisation permet d'esquisser un modèle général des systèmes complexes [Checkland, 1999 ; Leveson, 2006], où un niveau est caractérisé par ses *propriétés émergentes*, qui n'existent pas à un niveau inférieur et n'ont donc aucune signification à un autre niveau. En effet, les propriétés d'un système proviennent directement des interactions entre les différents éléments d'un système [Ackoff, 1971].

La sécurité est clairement une propriété émergente des systèmes [Leveson, 2006]. Déterminer si une installation industrielle est acceptablement sûre s'avère impossible sur la foi du seul examen de sa tuyauterie. La sécurité doit donc être placée dans un contexte et ne peut être déterminée qu'à partir des relations avec l'ensemble des éléments d'une installation ou d'une organisation. Il n'est donc pas possible d'isoler un élément et d'évaluer sa sécurité, car un élément parfaitement sûr dans un système peut ne pas l'être dans un autre.

La théorie de la hiérarchie traite quant à elle des différences entre un niveau de complexité et les autres. Elle cherche principalement à expliquer les liens entre les différents niveaux, c'est-à-dire ce qui les génère, les sépare ou bien les relie. Les propriétés émergentes associées avec un ensemble d'éléments à un niveau dans une hiérarchie influent sur le degré de liberté de ces éléments. Ainsi, décrire les propriétés émergentes résultant de l'application de contraintes requiert une analyse à un niveau supérieur, différent de celui décrit pour les éléments. Plusieurs propriétés peuvent donc apparaître au sein des systèmes complexes.

La conception de systèmes socio-techniques a pour but d'assurer la production tout en gérant le risque. Les différents niveaux sont soumis à des contrôles ainsi que les activités des opérateurs interagissant avec le processus sous contrôle. Les facteurs de niveau stratégique interagissent avec le niveau opérationnel. Le niveau stratégique d'un groupe est soumis aux différents textes réglementaires ou aux organisations professionnelles de son secteur d'activité. Cette organisation peut se poursuivre jusqu'au niveau gouvernemental. Ces influences dictent la loi de comportement du système.

Dès qu'un système fonctionne, les décisions prises à ses niveaux supérieurs se propagent dans les niveaux inférieurs (figure 6). Rétroactivement, les informations relatives aux actions des niveaux inférieurs peuvent remonter le long de la hiérarchie. Cette rétroaction est cruciale pour le bon fonctionnement du système, car si les décisions prises à un niveau supérieur ne sont pas transmises aux niveaux inférieurs, protéger le système de certains états dangereux s'avère difficile. Inversement, si les informations provenant du niveau « tactique » ne sont pas transmises aux niveaux supérieurs, les décisions ne pourront pas tenir compte de l'information disponible et des contraintes auxquelles le système fait face. Dans ce cas, le système peut devenir instable et commencer à migrer vers un niveau dangereux en raison d'une perte de contrôle du processus aléatoire qu'il a pour objet de contrôler. C'est précisément pourquoi, dans les systèmes socio-techniques, la sécurité est considérée comme une propriété émergente.

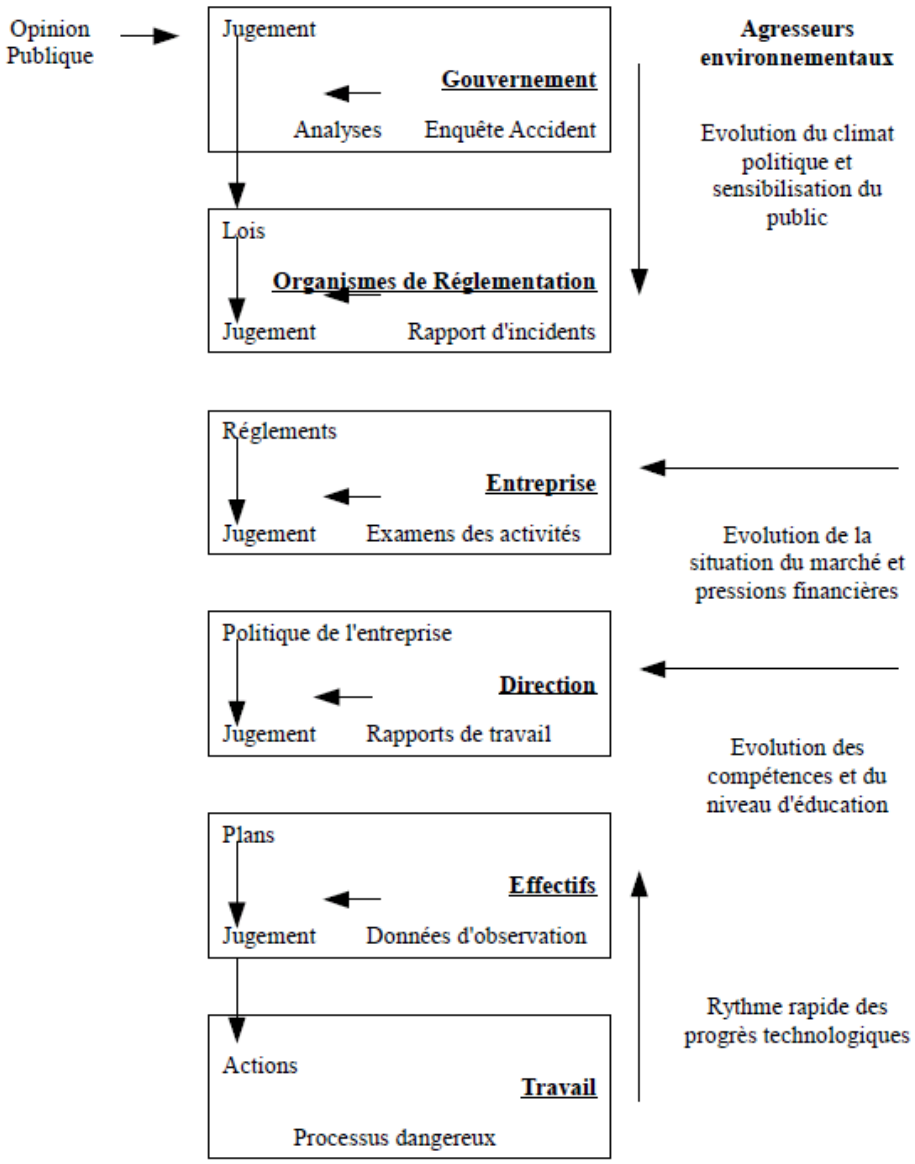


Figure 6 ■ Structure du système socio-technique
adapté de Rasmussen [Rasmussen, 1997]

Dans ce cadre, les atteintes à la sécurité prennent leur origine dans la perte de contrôle causée par l'application de contraintes inadéquates entre les niveaux du système et non pas seulement en raison de défaillances à un niveau précis. Chaque niveau joue donc un rôle dans le maintien de la sécurité, bien que ce rôle diffère d'un niveau à l'autre. La plupart du temps, une absence de rétroaction empêche toute appréhension globale du système et la prévention des menaces pesant sur la sécurité devient malaisée.

2.1.2. La composante dynamique

La seconde composante de l'analyse des accidents tient compte de l'aspect dynamique ; un système socio-technique évolue en effet au cours du temps et modifie sa structure [Rasmussen, 1997 ; Rasmussen, 2000]. Cette dynamique est soumise à différentes influences externes, susceptibles de pousser les éléments du système à modifier leur comportement — en obligeant par exemple les opérateurs à travailler aux limites du système et parfois à s'écarter des procédures en réagissant aux demandes et aux exigences de plus grande performance. Cet écart de procédure provoque la dégradation progressive des défenses. Plus pernicieux : cette déviation s'avère même *nécessaire* pour remplir certaines tâches au regard du stress subi au sein du système. Toutefois, de tels écarts ne mènent pas systématiquement à l'accident. À chaque niveau de la hiérarchie, les opérateurs travaillent dans un souci de performance mais n'ont pas forcément connaissance des décisions prises aux autres niveaux de la hiérarchie. Or, c'est précisément l'incoordination des décisions qui mène le système à l'accident [Rasmussen, 1997]. Ainsi, les opérateurs travaillent de plus en plus aux limites de la sécurité sans pour autant avoir conscience qu'ils confinent aux frontières du système. C'est pourquoi, dans les systèmes socio-techniques, les accidents découlent de la combinaison d'un déplacement systématique du travail et d'un évènement révélant la dégradation de la sécurité qui s'est produite durant toute cette migration et qui mène le système vers un état accidentel.

2.2. L'état accidentel

La notion d'« état accidentel » est directement issue de la théorie des systèmes et de la dynamique des systèmes. Un état accidentel[2] est considéré comme le résultat d'un phénomène accidentel se traduisant par une nouvelle configuration systémique caractérisée par une transition de phase de ses processus, de sa structure et/ou de sa fonction, dans un contexte donné se traduisant par une dégradation du système. Dans le cas d'un état accidentel, le système est dans un état excité dû à des perturbations intérieures et/ou extérieures. L'accident[3] est donc un phénomène dynamique émergent au sein d'un système et se caractérisant par des réponses (rétroactions) inadéquates face à une perturbation touchant l'équilibre oscillatoire d'un système, pouvant mener à des dommages et/ou à des pertes. Cette transition (dégradation) peut toucher indépendamment les processus, la structure et la fonction du système tout en ayant des conséquences sur ces trois caractéristiques en raison de leur interdépendance et de leurs interactions. C'est pourquoi, dans un contexte

2 Le concept de « crise » pourrait également être défini comme un état accidentel.

3 Notion qui peut être différenciée de celles d'incident et de catastrophe, notamment dans le degré de dommages et de pertes.

donné, la dégradation d'un processus a des répercussions sur l'ensemble du système et affecte aussi bien sa structure que sa fonction.

Les systèmes socio-techniques sont toujours dynamiques et non linéaires ; dans un souci de clarté, il semble toutefois plus simple d'illustrer la notion d'état accidentel en adoptant une démarche intégrable.

Comme souligné précédemment, au sein d'un système, les processus, la structure et la fonction sont liés (figure 7). Ainsi, dans les processus systémiques, tout changement — par exemple une action de contrôle inadéquate—, induit une modification de la structure du système (figure 7a) et donc de son comportement. Cette modification de comportement altère donc l'objectif même du système et sa fonction si aucune réponse n'est fournie à temps par le système (figure 7b). *A contrario*, toute variation (de la performance) dans la fonction retentit sur la structure et sur la hiérarchie du système, se traduisant par une modification des actions de contrôle et donc par une variation (de la performance) dans les processus. Toute perturbation du système provoque donc un effet oscillatoire sur le système ayant des conséquences diverses. Ainsi, des perturbations de petite amplitude n'ont qu'un impact limité et induisent une réponse linéaire de faible amplitude de la part du système.

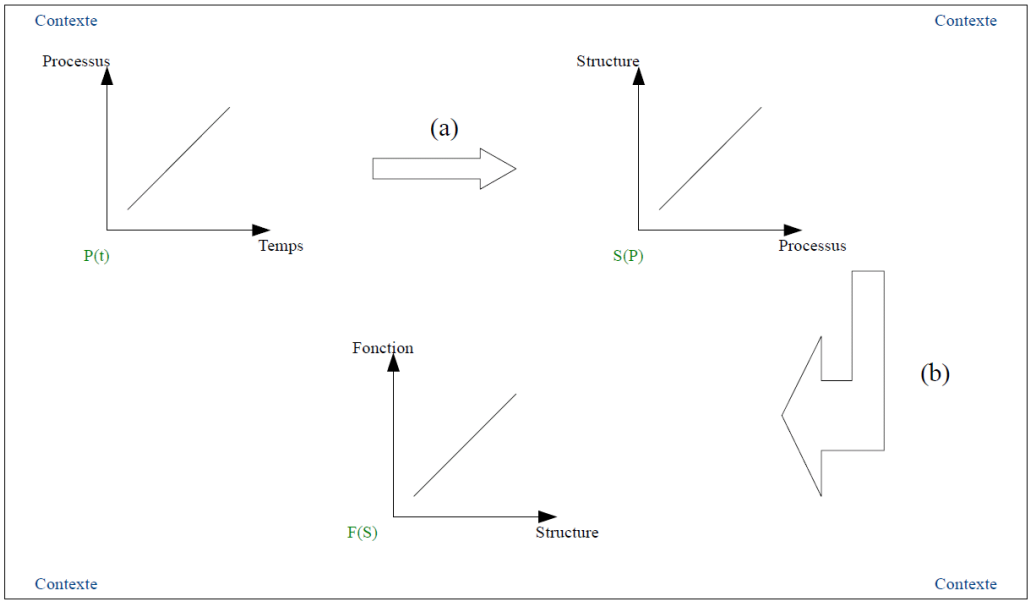


Figure 7 ■ Dépendance linéaire (sans réponse) des caractéristiques d'un système, basée sur la dégradation des processus.

Il est ainsi possible de représenter ces variations aussi bien dans une vision processuelle, aussi bien que structurelle ou fonctionnelle.

Si aucune réponse ou aucun contrôle n'est apporté de la part du niveau supérieur à un niveau en cours de dégradation, le système migre vers un état dangereux, voire vers sa désintégration. Cette réponse doit notamment se traduire par une action de

contrôle du niveau supérieur sur le niveau concerné en réponse aux informations qui sont transmises par les niveaux inférieurs.

Ce phénomène est susceptible de se propager vers le niveau le plus élevé du système, engendrant une migration de l'ensemble du système vers un état dangereux — c'est alors l'intégrité complète du système qui est en jeu.

En poursuivant notre raisonnement linéaire par souci de simplicité, l'état accidentel d'un système dépend donc directement de la dégradation de ce même système dans un contexte donné.

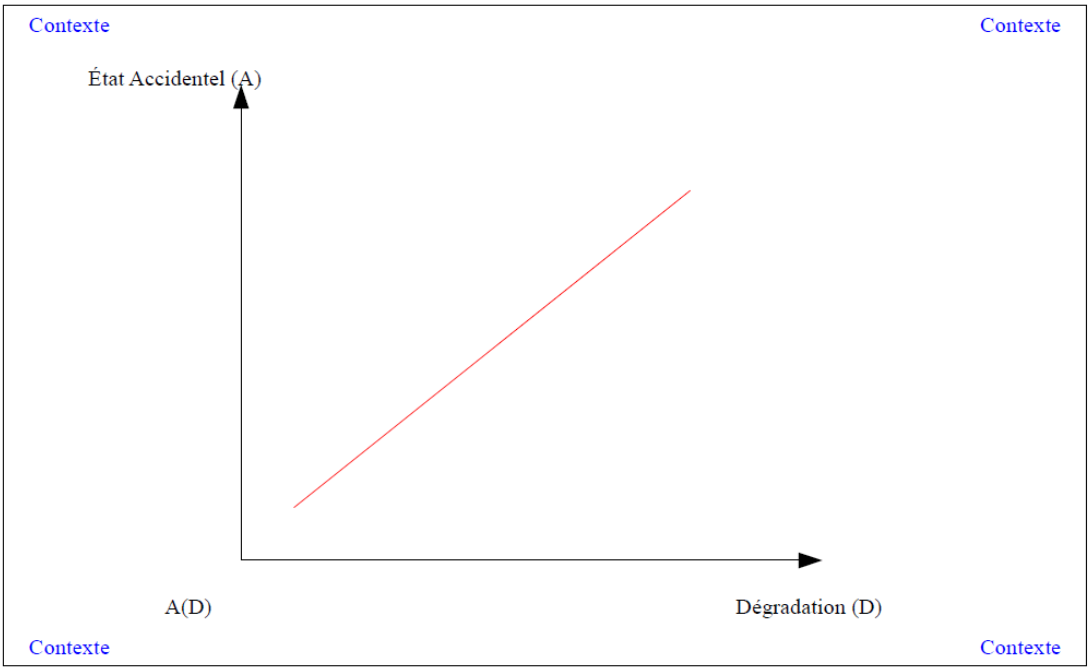


Figure 8 ■ Représentation linéaire (sans réponse) de l'état accidentel du système en fonction de sa dégradation.

Il est donc possible de définir trois types d'état accidentel en fonction du processus de migration :

- si des changements dans les processus sont la source d'une migration du système vers un état dangereux, cet état est qualifié d' « état accidentel par les processus » ou de « migration par les processus » ;
- en cas de migration due à une modification au niveau de la structure, cet état est qualifié d' « état accidentel structurel » ou de « migration structurelle » ;
- enfin, une migration due à un changement au niveau de la fonction définit l' « état accidentel fonctionnel » ou « migration fonctionnelle ».

Dans ce cadre, lorsqu'aucune réponse n'est apportée, la migration des processus est telle que le système entre dans un état accidentel, conduisant inéluctablement à une destruction du système par les processus. S'ensuit une migration de la structure

et de la fonction de l'état dangereux vers l'état accidentel menant au final à une destruction complète du système. Cette évolution, schématisée dans la figure 9, peut également s'expliquer par de fortes perturbations obligeant le système à sortir de son état de repos[4] l'emmenant vers un état excité et donc accidentel pour enfin passer dans un état de rétablissement avant de retrouver un état de repos. Ces perturbations peuvent se propager tout au long de la chaîne hiérarchique, qu'elles proviennent de la base, du sommet, de l'intérieur ou de l'extérieur du système.

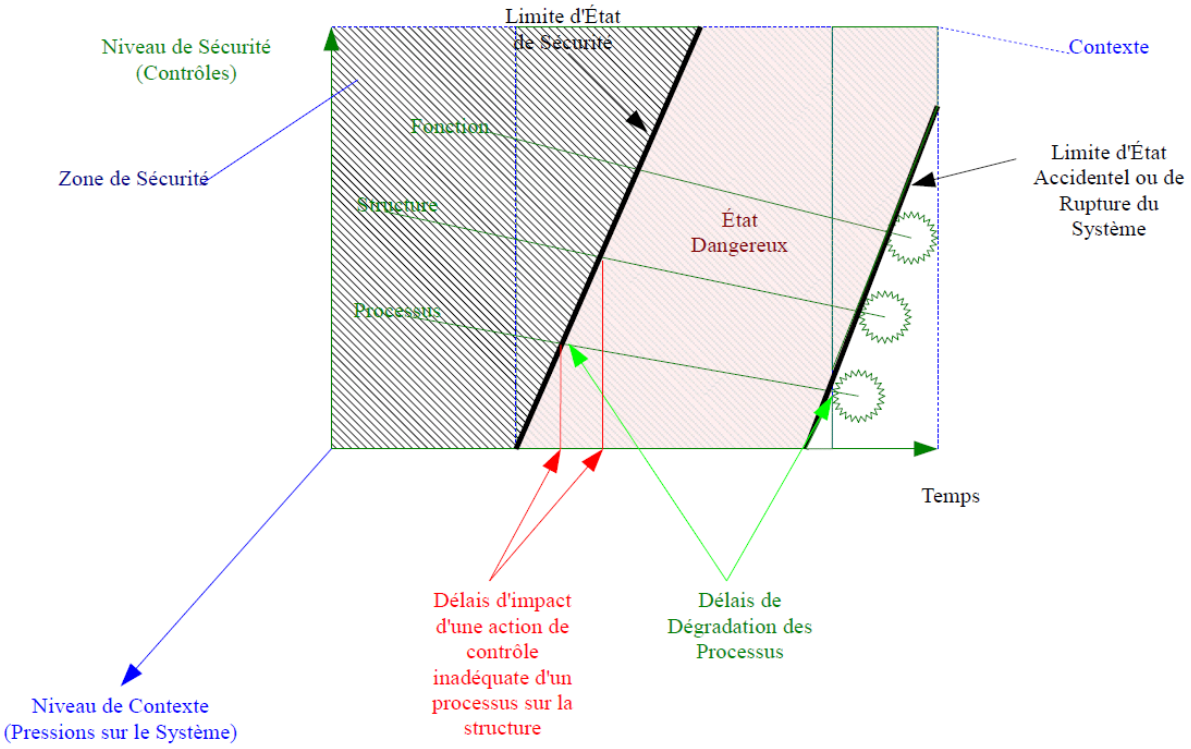


Figure 9 ■ Représentation linéaire de l'état accidentel dû à la migration par les processus d'un système complexe dans un contexte donné

La figure 9 montre, entre autres, la prise en compte des délais de dégradation dans cette représentation linéaire simplificatrice. Ces délais de dégradation — et donc de migration du système vers l'état dangereux — mettent en exergue l'entrée différée de la structure puis de la fonction dans cet état dangereux, voire dans l'état accidentel. La migration de l'ensemble des caractéristiques d'un système est donc progressive si aucune réponse (contrôle) n'est fournie au système dans des délais impartis. En effet, *les trois types de migration ne sont jamais simultanés*, excepté si une perturbation (interne ou externe) affecte le système dans sa globalité.

4 Si le système n'est pas perturbé, il reste dans un état de repos ou d'équilibre caractérisé par une stabilité comportementale.

Naturellement, plusieurs configurations peuvent exister selon que cette migration affecte la structure ou la fonction. Ces délais revêtent une importance capitale dans la prévention des accidents au sein des systèmes complexes et de la gestion des actions de contrôle inadéquates. En effet, plus un système complexe tarde à fournir une réponse à une action de contrôle inadéquate, plus sa propension est forte à migrer vers un état dangereux. De façon générale, les délais ont une forte influence sur le comportement général d'un système et toute modification de la durée d'un délai peut avoir des répercussions sur le système global — par exemple, le temps de réponse du système face à une perturbation (interne ou externe). Un délai est donc source de dangers en créant une instabilité et des oscillations dans un système donné. Omniprésents [Sterman, 2000], les délais sont à l'origine d'une prise de temps pour mesurer ou répercuter de l'information, ou encore pour prendre une décision. Les délais peuvent aussi bien être d'ordre matériel qu'informationnel.

Il est donc possible de définir l'« état systémique sûr » comme l'état du système pour lequel ses caractéristiques se trouvent dans la zone de sécurité, donc hors de tout état dangereux et *a fortiori* de tout état accidentel.

Dans un système complexe, la gestion des états accidentels se traduit par une gestion des actions de contrôle au niveau des processus, de la structure et de la fonction du système, gestion recourant notamment à la modélisation de l'accident.

Dans les systèmes socio-techniques, l'accident est non linéaire, c'est-à-dire qu'il est le résultat d'un phénomène dans lequel la réaction est disproportionnée à l'action. Or, cette non-linéarité rend toute prédiction accidentelle extrêmement difficile : dans un système non linéaire, les erreurs s'amplifient en effet rapidement et une incertitude infinitésimale dans l'état présent d'un système rend nulle toute prédiction de son état au delà d'un laps de temps. C'est cette propriété de non-linéarité dans le système qui permet de produire des structures émergentes et de générer une dynamique au sein d'un système. Un système dynamique non linéaire n'a pour point d'équilibre aucun point fixe : son équilibre est une série d'états que le système parcourt pour conserver ses caractéristiques (processus, structure, fonction) tout en évoluant sans cesse. L'état accidentel fait partie de ces états systémiques. Ainsi, c'est l'agitation permanente et l'instabilité au sein de ce système, le désordre et la variation qui produisent l'ordre et la conservation. Dans l'analyse de sécurité de tout système dynamique, la structure étudiée à un instant donné est produite par la dynamique même du système, résultant elle- même des interactions positives (boucles explosives) et négatives (boucles négatives). Dans les systèmes socio-techniques pourvus de couplages forts existent des mécanismes dynamiques capables de s'autoréguler afin de produire une structure stable et non accidentelle. Cette stabilité (ou cette sensation de sécurité) peut perdurer suffisamment longtemps pour sembler constante. Puis, du fait d'un petit changement, les boucles de rétroaction sont susceptibles de se désordonner et même de sauter rapidement à un autre état d'équilibre. C'est pourquoi la migration d'un système vers un état accidentel représentée dans la figure 9 différera, dans le cas des systèmes socio-techniques, en

raison de ces rétroactions au cours du temps : la migration perd alors son caractère linéaire, et l'observateur se trouve alors bel et bien confronté à une migration du système dans sa globalité. Ainsi, l'étude d'accidentogénicité d'un système dynamique non linéaire ne passe pas exclusivement par une compréhension des interactions entre éléments mais aussi par la compréhension des propriétés des interactions entre les éléments (durée, rythme, fréquence…).

Par conséquence, l'analyse de l'état accidentel d'un système dynamique non linéaire impose d'en comprendre la structure s'il est doté de propriétés émergentes résultant des interactions internes sous l'influence des échanges avec son environnement. Ces propriétés émergentes sont celles de la fonction du système. Ainsi, dans les systèmes dynamiques non linéaires tels que les systèmes socio-techniques, il est important de comprendre la structure même du système *mais sans s'y cantonner*[5]. Cette démarche de compréhension structurelle passe par la constitution de « modèles d'accident systémiques », qui permettent d'analyser la structure émergente d'un système et par conséquent sa sécurité, propriété émergente issue de l'interaction des éléments entre eux.

Cette modélisation constitue une réponse aux insuffisances des modèles d'accident, fondés sur l'approche analytique, et des approches organisationnelles du risque, ne prenant pas en considération l'aspect dynamique non linéaire d'un système. Tel est l'objet du paragraphe suivant, qui présente les modèles d'accident systémique en s'intéressant plus particulièrement à deux d'entre eux : les modèles FRAM [Hollnagel, 2004] et STAMP [Leveson, 2003].

3. Les modèles d'accident systémiques

Les technologies modernes ont un retentissement important sur la nature même des accidents, imposant de mettre en place de nouveaux mécanismes d'explication afin de les comprendre et de développer de nouvelles techniques d'évaluation des risques pour prévenir leur survenance [Leveson, 2003]. Ce besoin de nouvelles approches est illustré par Hollnagel, qui fournit une chronologie des changements intervenus dans la vision des accidents depuis les années 1950 au regard d'une nouvelle compréhension de la nature des accidents [Hollnagel, 2001].

5 Le chapitre 5 présentera quelques perspectives, notamment l'intégration de la prise en compte du chaos (déterministe) dans la compréhension des accidents. En effet, les systèmes non chaotiques ne constituent qu'une catégorie particulière de systèmes (par exemple les systèmes hamiltoniens). L'état accidentel, dans de tels systèmes, pourrait être caractérisé comme une transition de phase, c'est-à-dire comme un saut qualitatif brutal et dans lequel la structure du système change de manière discontinue, passant d'un état non accidentel à un état accidentel. Plus aucune limite ne sépare un état de sécurité ou un état sûr d'un état accidentel car la transition entre ces deux états est une réorganisation du système (due par exemple à une perturbation) provoquant un réaménagement de ses éléments et engendrant ainsi de nouvelles propriétés et de nouveaux comportements.

Les modèles d'accident systémiques permettent de mieux décrire et de mieux comprendre les liens entre les différents facteurs à travers différents niveaux hiérarchiques ; ils facilitent ainsi l'étude de problèmes que seule rend possible la vision globale d'un système socio-technique.

Les modèles systémiques d'accident se distinguent des autres modèles par la description qu'ils permettent du processus d'accident comme un ensemble d'évènements interconnectés et complexes, alors que les modèles séquentiel et organisationnel se contentent d'une description linéaire de l'accident. Dans les modèles systémiques, un accident survient lorsque plusieurs facteurs (humain, technique, environnemental) coexistent en un lieu et un temps spécifique [Hollnagel, 2004].

Les modèles de sécurité fondés sur la théorie des systèmes voient les accidents comme des phénomènes émergents résultant des interactions entre les éléments d'un système dont les interactions sont non linéaires et pourvu de nombreuses boucles de rétroaction [Perrow, 1984]. En effet, la sécurité n'est établie que par les interactions entre les éléments d'un système et ne constitue pas la propriété individuelle d'un élément. Les modèles systémiques puisent donc leur source dans la théorie des systèmes, ses principes, ses modèles et les lois qu'elle propose pour la compréhension des relations entre les éléments d'un système complexe. Par conséquent, un système n'est pas vu selon une conception statique, mais comme un processus dynamique en continuelle adaptation afin d'atteindre ses objectifs et répondre aux changements internes et externes.

Les modèles d'accident systémiques ont pour objectif de considérer le caractère dynamique non linéaire d'un système et la migration d'une organisation sous contraintes vers un état dangereux voire accidentel. La proactivité de ces modèles d'accident en matière de prévention des risques permet d'aborder les problèmes affectant de façon globale le système plutôt qu'en mettant l'accent sur des problèmes spécifiques associés à des erreurs isolées, considérées hors du contexte dans lequel elles ont été effectuées. Ce type de modèle prend également en considération l'aspect dynamique en modélisant cette migration au sein des organisations subissant certaines pressions globales et environnementales. Rasmussen précise que la production et l'effort poussent les acteurs vers des niveaux supérieurs de risque en raison de changements progressifs dans la pratique [Rasmussen, 1997 ; Rasmussen, 2000]. Ces changements ne sont pas forcément néfastes au système s'ils sont associés à une adaptation face à la situation en augmentant par exemple la production.

L'aspect « dynamique » des systèmes, après l'aspect « hiérarchique », constitue la seconde composante du modèle d'accident systémique [Rasmussen, 1994 ; Rasmussen, 1997 ; Rasmussen, 2000 ; Rasmussen, 2002]. La dynamique des systèmes a quant à elle été développée par Jay Forrester à partir de la fin des années 1940 parallèlement à l'émergence de la sécurité des systèmes [Forrester, 1961 ; Forrester, 1969 ; Forrester, 1972 ; Forrester, 1973]. Les travaux de Forrester en dynamique des systèmes, appliqués à des systèmes économiques, sont aujourd'hui complétés par

ceux que Donella Meadows a développés ces trente dernières années sur les situations économique, environnementale et démographique mondiales [Meadows, 1972 ; Meadows, 1992 ; Meadows, 2004]. Signalons également les travaux de Peter Senge [Senge, 2006], professeur au Massachussets Institute of Technology, sur la pensée et l'analyse systémiques dans le cadre d'organisations apprenantes prenant en considération leur dynamique dans un souci de performance et d'intégration du changement.

Tout système complexe possède une dynamique propre, due à son évolution et à l'activité pouvant relier ses éléments. Cette dynamique est soumise au jeu des différents éléments, selon certaines règles et certains principes permettant un contrôle de l'état du système au cours du temps.

Le défi consiste, en matière de sécurité des systèmes, à toujours garder à l'esprit que les systèmes complexes sont dynamiques et que l'état de stabilité dynamique d'un système peut devenir un état d'instabilité dynamique — l'existence d'un état stable dynamique étant bien sûr utopique car un système dynamique ne se trouve jamais très longtemps dans un état stable !

Le contrôle s'opère au niveau des interactions entre les éléments et les différents contrôleurs et niveaux hiérarchiques du système. Les règles de la théorie du contrôle, décrites dans le chapitre 3, permettent de comprendre les influences potentielles et d'appréhender les jeux de pouvoir à l'œuvre entre les éléments d'un système.

L'intégration des aspects cognitifs, mais aussi hiérarchiques et dynamiques des systèmes trouve sa traduction dans les travaux d'Erik Hollnagel qui, à partir d'une approche cognitive, développe la notion de dégradation de la performance d'un système, menant à l'accident, ainsi que dans les travaux de Jens Rasmussen présentant un cadre socio-technique hiérarchique [Rasmussen, 1997] et dans le modèle STAMP (*Systems-Theoretic Accident Model and Processes*) de Nancy Leveson [Leveson, 2004]. Le modèle STAMP, qui se fonde sur la théorie des systèmes et sur la théorie du contrôle, fait l'objet du chapitre 3.

3.1. L'approche d'Hollnagel

L'approche systémique des accidents a vu se développer de nouvelles approches de modélisation des accidents adoptant une vision systémique qui appréhende la performance d'un système comme un tout. Les progrès techniques soutenus opérés depuis quelques décennies ont profondément modifié la nature du travail humain, et les tâches hier manuelles allient aujourd'hui activités intensives et tâches cognitives. Les approches centrées sur les technologies ont conduit à l'émergence de problèmes spécifiques en matière de performance opérationnelle et de nouveaux types de défaillances dans les systèmes homme-machine. Ces bouleversements ont eu pour conséquences de nombreuses catastrophes dans les domaines de l'aviation, du nucléaire ou de la défense [Parasuraman, 1997].

En 1983, l'apparition de l'ingénierie cognitive [Hollnagel, Woods, 1983] fournit un cadre innovant de modélisation du comportement des systèmes homme-machine en contexte opérationnel. L'ingénierie cognitive précise qu'il n'est pas possible de comprendre ce qui ce passe quand les choses vont mal sans comprendre ce qui se passe lorsqu'elles vont bien [Hollnagel, Woods, 2005]. Hollnagel et Woods introduisent un nouveau paradigme privilégiant le concept central de « système cognitif conjoint », où l'homme et la machine fonctionnent parallèlement et abandonnant l'approche fondée sur l'interaction homme/machine.

Deux modèles d'accident systémiques, destinés à la sécurité et à l'analyse des accidents, ont été développés à partir des principes de l'ingénierie des systèmes cognitifs :

- la méthode CREAM (*Cognitive Reliability and Error Analysis Method*) permet, à partir de la modélisation des aspects cognitifs de la performance humaine, d'évaluer les conséquences des erreurs humaines sur la sécurité d'un système [Hollnagel, 1998]. Deux variantes de cette méthode existent [Hollnagel, 2006] : DREAM (*Driver Reliability and Error Analysis Method*), pour l'analyse des accidents de trafic, et BREAM (*Bridge Reliability and Error Analysis Method)*, pour l'analyse des accidents maritimes ;
- la méthode FRAM (*Functional Resonance Accident Model*) est un modèle d'accident qualitatif décrivant les modalités selon lesquelles les fonctions des éléments d'un système peuvent entrer en résonance et créer des dangers pouvant mener à une perte de contrôle, donc à un accident [Hollnagel, 2004]. FRAM est basée sur la notion de variabilité de la performance, la variabilité interne ou externe étant normale puisque la performance n'est, dans les systèmes socio-techniques, jamais stable.

3.2. L'approche de Rasmussen

Le cadre socio-technique de Jens Rasmussen est caractérisé par deux composantes permettant de répondre au développement des systèmes socio-techniques, gérés par des organisations opérant dans des environnements extrêmement volatils et dynamiques tels que l'économie de marché, les pressions économiques et politiques, la réglementation ou l'augmentation de la prise de conscience sociale de la sécurité [Rasmussen, 1997]. Rasmussen souligne que ces conditions ont modifié le caractère dynamique de la société moderne et influencent de façon continue les procédures de travail et le comportement humain lors de l'exploitation des systèmes complexes.

L'approche systémique permet à Rasmussen de modéliser les structures opérationnelles, de management et organisationnelles susceptibles de créer un cadre accidentel. Ce cadre comprend deux composantes : la première est une hiérarchie de la structure ; la seconde prend en considération la dynamique du système à mesure qu'il migre vers sa limite de sécurité.

3.2.1. La structure hiérarchique

Pour Rasmussen, la gestion des risques est un problème de contrôle du système socio-technique dans lequel les blessures, la contamination de l'environnement ou la perte d'investissement surviennent en raison d'une perte de contrôle des processus.

Dans le fonctionnement « normal » d'un système, les décisions des niveaux supérieurs descendent le long de la hiérarchie vers les niveaux inférieurs. Parallèlement, les informations sur l'état des niveaux inférieurs doivent remonter la hiérarchie. Ce double sens de circulation des flux est primordial pour l'équilibre du système. Le système socio-technique inclut plusieurs niveaux hiérarchiques allant du législateur au simple opérateur.

La sécurité dépend du contrôle des processus de travail et doit par conséquent chercher à éviter les effets indésirables causant des dommages aux individus, à l'environnement ou à l'investissement [Rasmussen, 1997].

Si l'information de base n'est pas transmise aux niveaux supérieurs, les décideurs ne peuvent pas tenir compte de la capacité disponible, des limites du système ou des contraintes auxquelles celui-ci fait face. Il en résulte une possible instabilité du système, donc une perte de contrôle du processus qu'il a la charge de contrôler. La sécurité est donc bien une propriété émergente d'un système socio-technique. De ce point de vue, un accident peut avoir pour origine une perte de contrôle causée par une absence d'intégration verticale ou une mauvaise communication entre les différents niveaux du système socio-technique. Chaque niveau joue donc un rôle dans le maintien de la sécurité d'un système. Ainsi, lorsque plusieurs niveaux sont soumis à des contraintes ou à des pressions à différents moments, il est important que les démarches d'amélioration de la sécurité à un niveau prennent en compte ces changements imposés par les autres niveaux.

3.2.2. La dynamique du système

La dynamique du système constitue la seconde composante de l'approche de Rasmussen. Dans les environnements complexes il est impossible de mettre en place des procédures pour chacune des situations potentielles, en particulier en cas d'urgence, de haut risque ou de situation inattendue [Rasmussen, 1997]. La dynamique tient compte des influences dynamiques pouvant modifier la structure du système, donc son comportement.

Pour maintenir le niveau de sécurité d'un système socio-technique, il est essentiel que les décisions prises et les activités humaines restent dans les limites de travail définis par les contraintes administratives, fonctionnelles et de sécurité. Rasmussen souligne qu'il est important d'identifier les limites de sécurité ainsi que les influences dynamiques pouvant faire migrer le système socio-technique vers ou en dehors de ces limites. Cet espace de liberté dans lequel tout élément du système socio-technique peut naviguer est délimité par trois frontières :

- une charge (psychologique) acceptable de travail ;
- des contraintes économiques et acceptables ;
- des procédures et des réglementations de sécurité.

Chacune de ces frontières est susceptible de produire un gradient influençant le système. Par exemple, les pressions financières sont à l'origine d'un gradient de coût ayant une influence sur le comportement individuel provoquant une adaptation économique des stratégies de travail. Une charge de travail supplémentaire crée un gradient motivant les individus à modifier leurs pratiques de travail afin de réduire le travail physique et cognitif. Ces différents gradients sont à l'origine d'une variation aléatoire (ou brownienne) du comportement humain.

Chacune de ces variations peut mener les éléments à s'écarter des procédures et à provoquer des dégradations des défenses du système. De plus, ces variations n'ont pas forcément des conséquences visibles et immédiates. Malheureusement, ces comportements adaptatifs poussent progressivement les opérateurs à franchir les limites ainsi que le système dans sa globalité. L'accident est inévitable si le contrôle n'est pas maintenu à la limite.

La structure de contrôle de la sécurité elle-même change au cours du temps et peut migrer vers les limites de sécurité ; un unique évènement ou une infime déviation peut alors provoquer une catastrophe.

L'étude d'accidents comme Bhopal ou Tchernobyl a montré que ces catastrophes ne sont pas le résultat d'une unique défaillance humaine ou organisationnelle, mais la conséquence d'une migration du comportement organisationnel vers l'accident sous l'influence de pressions financières dans un environnement extrêmement compétitif [Rasmussen, 1997].

L'approche de Rasmussen permet donc de délimiter un champ d'opérations sûres, le rendant visible pour les acteurs et permettant de contrôler son comportement au sein de ces limites.

Cette approche systémique a profondément influencé les travaux de Nancy Leveson, professeur au MIT qui a pu mettre en place un nouveau modèle d'accident appelé STAMP (*System-Theoretic Accident Modeling and Processes*), présenté au chapitre 3.

Conclusion

Ce chapitre a présenté l'accident comme un phénomène émergent systémique, dépassant les approches l'analysant comme un évènement linéaire en bout de chaîne ou comme l'aboutissement de multiples défaillances de défenses dans un système.

L'approche systémique de l'accident vise à répondre aux limites des modèles d'accident linéaires en tenant compte du caractère dynamique non linéaire du comportement de tout système.

Dans cette optique, ont d'abord été présentées la systémique et la pensée système afin de cerner les fondements de la théorie des systèmes. L'accident survenant au sein des systèmes a ensuite été appréhendé par une présentation de la notion d'état accidentel.

Ce chapitre se termine donc par les modèles d'accident systémiques, et notamment par le cadre socio-technique de Rasmussen, qui sert partiellement de cadre au modèle d'accident STAMP, objet du chapitre suivant.

Chapitre 3
Le modèle d'accident STAMP

L'ambition de repousser les limites des modèles d'accident « traditionnels » et de tenir compte des interactions dans les systèmes socio-techniques modernes conduit à recourir à un modèle capable de représenter l'ensemble des changements systémiques, en y associant l'idée que les accidents sont le résultat d'un « contrôle inadéquat »[6] menant le système vers un état accidentel.

Le modèle d'accident STAMP (*System-Theoretic Accident Modeling and Processes*)[7] a été développé par Nancy Leveson [Leveson, 2004 ; Leveson, 2006 ; Hollnagel, Woods, Leveson, 2005] et intègre cette notion de « contrôle inadéquat ». Il permet d'établir à la fois des structures statiques et dynamiques, outils visant à identifier, à analyser et à évaluer toute migration d'un système vers un état accidentel. Il décrit l'accident comme un processus d'évolution systémique, et non comme une chaîne d'évènements, dans lequel les contraintes en sécurité des systèmes sont appliquées de façon inadéquate en conception, en développement ou durant l'exploitation d'un système [Dulac, 2007].

Ce chapitre présente d'abord les fondements du modèle STAMP développés à partir de la théorie des systèmes (*v.* chapitre 2, notamment les notions de processus, de structure, de fonction et de contexte) et la théorie du contrôle. Les trois principaux concepts (la contrainte, la structure de contrôle, les modèles de processus) du modèle STAMP sont ensuite décrits. Enfin est exposée la technique d'analyse des dangers STPA, construite à partir du modèle d'accident STAMP et visant à analyser les accidents ou à évaluer le niveau de sécurité dans un système.

6 Ce contrôle inadéquat se traduit par l'application de contraintes de sécurité ne permettant pas le maintien d'un niveau de sécurité acceptable.

7 Modélisation et processus des accidents systémiques.

1. Les fondements théoriques du modèle STAMP

Le modèle d'accident STAMP repose à la fois sur la théorie des systèmes et la théorie du contrôle.

La théorie des systèmes — tout comme la théorie du contrôle et la sécurité des systèmes — a fait l'objet d'une présentation approfondie dans le chapitre 2 : « la théorie des systèmes a été développée après la Seconde Guerre mondiale afin de faire face à l'importante augmentation de la complexité des systèmes, particulièrement des systèmes militaires. Dans la théorie des systèmes, les systèmes sont vus comme des éléments interreliés maintenant un état d'équilibre dynamique par le biais de boucles de rétroaction d'informations et de contrôles. Les systèmes ne sont pas traités comme une conception statique mais comme un processus dynamique qui est continuellement adapté afin d'atteindre son but et de réagir face aux modifications internes et de leurs environnements. Pour être sûre, la conception originale ne doit pas seulement renforcer les contraintes sur le comportement pour assurer des opérations sûres (c'est-à-dire en renforçant les contraintes en sécurité des systèmes), mais le système doit continuer à fonctionner de façon sûre lorsque des modifications et des adaptations surviennent au cours du temps afin d'atteindre l'ensemble des buts et valeurs complexes évoluant à partir de conditions sociales et techniques » [Leveson, 2006]. Cet aspect dynamique des systèmes complexes doit donc une nouvelle fois être souligné.

Insister sur la théorie du contrôle permet, pour sa part, de rappeler les fondements théoriques du modèle d'accident STAMP. Cette théorie repose principalement sur le concept de rétroaction car dans aucun système complexe, un mécanisme naturel ou technologique n'est plus présent. Grâce aux boucles de rétroaction, une centrale nucléaire maintient la température de son cœur constante même lorsque la température ambiante peut varier de plusieurs dizaines de degrés ; grâce aux boucles de rétroaction, un avion peut maintenir son cap, son altitude et sa vitesse, peut également décoller sans aucune intervention humaine, et simplement ; grâce aux boucles de rétroaction encore, dans le domaine économique, la Réserve fédérale américaine exerce son autorité afin de stabiliser l'économie, par un jeu subtil de rétroactions et de contrôles.

Dans ce courant théorique, le mot « contrôle » prend une acception différente de son utilisation quotidienne. Dans le contexte d'individus, de groupes ou d'organisations, une personne parlant de « contrôle » pense souvent à la notion de coercition ou de dominance comme dans les structures organisationnelles hiérarchiques de « commandement et de contrôle », de type militaire par exemple. La théorie du contrôle fut initialement développée dans le but de concevoir des outils d'analyse et de contrôle de systèmes ; cette ingénierie du contrôle peut être lue comme l'utilisation intentionnelle du mécanisme de rétroaction afin de contrôler le comportement d'un processus dynamique [Belanger, 1995]. Cet aspect de l'ingénierie

du contrôle des systèmes est généralement appelé « théorie du contrôle ». Le terme « théorie » est approprié pour plusieurs raisons :

- premièrement, il est essentiellement mathématique dans son contenu, et les mathématiques sont souvent confondues avec la théorie ;
- ensuite, cette théorie met en œuvre non un système réel, mais des modèles fonctionnant sous certaines conditions et n'étant qu'une représentation de la réalité ;
- enfin, elle est constituée d'un corpus de connaissances : théorèmes, algorithmes de conception, méthodes graphiques…

Cette présentation comporte quatre phases : la première expose les enjeux du contrôle ; la deuxième traite des moyens de contrôle au sein d'un système ; la troisième s'attache à introduire les conditions d'un contrôle ; la dernière introduit le contrôle dans le cadre plus spécifique de la sécurité.

1.1. Contrôler : une nécessité justifiée

D'une manière générale, plusieurs arguments justifient le besoin de contrôler un système ; quatre sont particulièrement importants : l'économie, la sécurité, la performance et la fiabilité [Bossel, 2007].

Les considérations économiques importent surtout dans le processus de contrôle, c'est-à-dire dans le contrôle des systèmes de production. Beaucoup de ces systèmes, appelés « processus continus », ont été conçus pour maintenir un état stable. Par exemple, les usines sont des processus continus conçus pour maintenir des conditions d'opérations constantes, sauf au démarrage et à l'arrêt. Ces processus sont souvent réglés afin d'atteindre le rendement économique maximal, soumis à des contraintes inégales imposées à certaines variables en termes de qualité ou de sécurité. Tel est souvent le cas lorsque la solution optimale demande un fonctionnement proche de la limite du système et pousse ce système vers un rendement maximal.

La sécurité revêt également une dimension capitale en termes de contrôle. Un avion n'a, au décollage, qu'une visibilité très réduite et doit donc être contrôlé afin de lui garantir une piste de décollage sûre ; un réacteur nucléaire doit fonctionner d'une telle façon que les variables principales soient maintenues dans des limites sûres de fonctionnement. La majorité des systèmes connaissent des zones de danger, dont le but des contrôles est de les éviter.

Un niveau de performance donné ne peut être atteint sans contrôles. Un avion doit posséder un système de contrôles pour atteindre la manœuvrabilité requise ; une centrale nucléaire doit être assez performante pour fournir l'énergie à une population. Cette production ne serait être efficace sans un contrôle adéquat.

Le contrôle est enfin utilisé pour atteindre une meilleure fiabilité. Soumis à des perturbations, les systèmes physiques sont habituellement sujets à des défaillances.

Ce besoin de fiabilité se traduit par l'application de redondances au sein des systèmes physiques pour pallier toute défaillance inopportune.

Par ailleurs, « contrôler » signifie « produire un effet délibéré sur l'état d'un système dynamique » [Ogata, 1997]. Dans le contexte des systèmes socio-techniques, le mot « contrôle » est associé au contrôle des personnes, donc aux concepts de « commandement et de contrôle ». Lorsqu'il est souhaitable de conserver une influence sur un potentiel de travail, le contrôle porte sur le comportement des personnes ou d'un groupe, et le concept de « commandement et de contrôle » se révèle approprié — ce qui n'est pas le cas lorsqu'il est nécessaire de contrôler la sécurité d'un système et la capacité d'une organisation à apprendre de ses erreurs [Carroll, 2002].

La théorie du contrôle cherche à identifier les variables d'état du système à contrôler et les moyens appropriés pour contrôler ces variables afin de maintenir le système à l'écart de tout danger, c'est-à-dire à l'écart de tout « état ou ensemble de conditions (d'un système (ou un objet)), pouvant mener inévitablement à un accident (évènement de pertes)) » [Leveson, 1995]. À partir de cette vision des dangers d'un système, le management des risques peut être appréhendé comme un problème de contrôle : l'état du système désiré et les contraintes sur le comportement du système pour maintenir le système dans cet état peuvent être identifiés et une structure de contrôle socio-technique peut être définie afin de mettre en œuvre les contraintes de sécurité d'un système [Leveson, 2004 ; Leveson et Dulac, 2005].

Lorsque, dans un système, l'état du système désiré est établi, c'est à la structure de contrôle d'entrer en jeu. Le système de contrôle convertit ainsi le but du système en actions devant être contrôlées afin d'atteindre un objectif ou de le maintenir. Pour ce faire, le système utilise des boucles de contrôle.

1.2. Les boucles de contrôle

On distingue les systèmes de contrôle selon qu'ils reposent sur des boucles ouvertes ou des boucles fermées (ou structures à contrôles par rétroactions).

1.2.1. Les boucles ouvertes

Le contrôle en boucle ouverte forme la structure de contrôle la plus simple. Limitée en performance, elle est habituellement réservée à des applications spécifiques dans lesquelles le contrôle par rétroaction s'avère soit impossible, soit inutile. En raison de sa simplicité, le contrôle en boucle ouverte constitue une base de départ idéale pour l'étude des structures de contrôle, même si ses limites doivent être connues. Des concepts tels que les conditions de stabilité et les limites de performance y apparaissent sous une forme relativement simple, mais qui peut considérablement se complexifier dans d'autres contrôles de structure. Un système

ouvert est donc caractérisé par des sortants répondant à des entrants mais dépourvus de toute espèce d'influence sur eux. Ce système n'a donc pas conscience de sa propre performance [Forrester, 1969]. Dans un système ouvert, les actions passées n'ont aucune influence sur les actions futures. Dans le cas d'une boucle de contrôle ouverte, l'observateur, s'il existe, n'a aucun retour d'information sur l'état du système provenant du contrôleur. Le contrôleur ne peut prendre en compte en temps réel les informations sur l'état du système. Par conséquent, il ne peut transmettre les actions à effectuer à l'actionneur (dispositif permettant d'agir sur un système) du système.

1.2.2. Les boucles fermées

Le système fermé (ou système à rétroactions) est soumis à son propre comportement passé. Un système à rétroactions a donc une structure à boucles fermées intégrant les résultats d'un comportement passé dans la prise de décisions futures. Un système est dit de premier ordre lorsqu'il ne contient qu'une variable d'état, et de second ordre lorsqu'il en contient deux. Ainsi, les systèmes de contrôle peuvent être constitués de boucles de rétroaction (figures 10 et 11) comportant différents éléments fondamentaux [Leveson, 2003 ; Leveson et Dulac, 2005 ; Leveson, 2006] :

- le *contrôleur* matérialise la logique du système de contrôle et détermine les actions de contrôle à effectuer au sein de ce système. Le contrôleur contient un modèle du reste du système, incluant les autres éléments de contrôle ;
- un *actionneur* est un élément physique ou un agent imposant la volonté du contrôleur sur le système en exécutant l'action de contrôle ;
- l'observateur (ou capteur) est l'élément du système de contrôle vérifiant l'état du système.

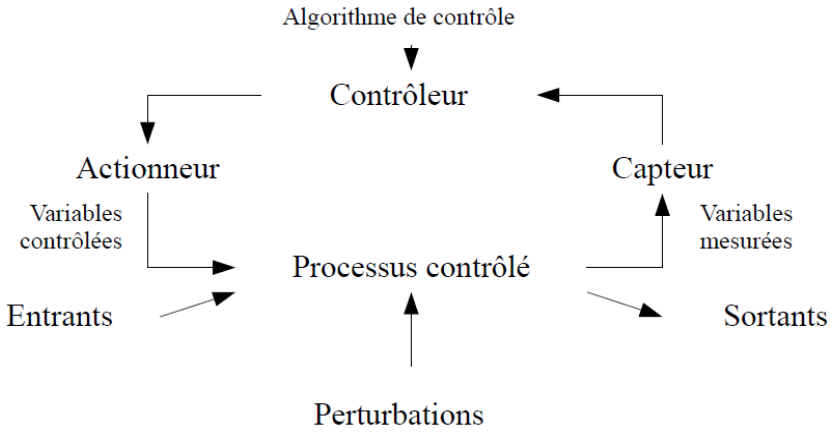


Figure 10 ■ Boucle de contrôle standard
adapté de Leveson [Leveson, 2005]

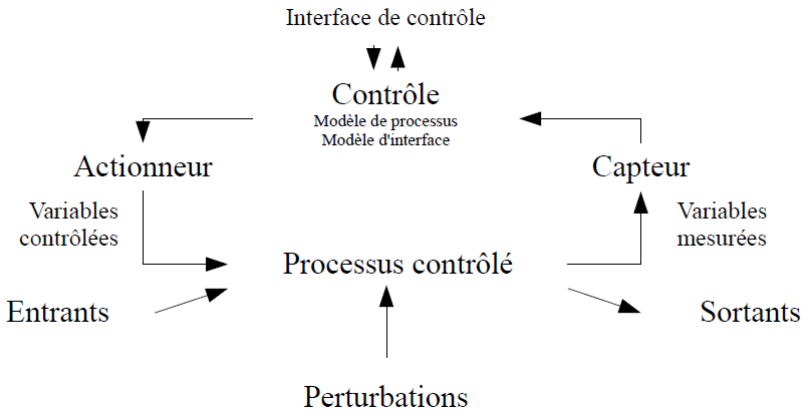


Figure 11 ■ Boucle de contrôle supervisée
adapté de Leveson [Leveson, 2005]

Dans le cas d'une boucle de contrôle fermée ou d'un contrôle par rétroaction, l'observateur fournit les informations sur l'état du système au contrôleur. Le contrôleur compare cette information avec l'objectif et détermine alors (à partir du modèle du système) une action de contrôle afin de repositionner l'état du système vers l'état désiré. Le contrôleur utilise l'information de l'observateur pour mettre à jour son modèle et modifier la manière de contrôler un actionneur.

Communication et contrôle forment donc une dyade de concepts indissociables dans la théorie des systèmes. L'intégration de contraintes sur une activité à un niveau de la hiérarchie définit une loi de comportement. Au sein des systèmes, les hiérarchies sont caractérisées par un processus de contrôle fonctionnant à l'interface des niveaux. En système ouvert, les contrôles induisent un besoin de communication, puisque le système est perçu comme une combinaison d'éléments interreliés maintenant un contrôle et un état d'équilibre dynamique grâce à boucles de rétroaction d'informations et de contrôles.

1.3. Les conditions de contrôle

Pour être pourvu d'effets sur l'ensemble d'un système, un contrôle doit généralement réunir quatre conditions [Leveson, 2006] :

- *une condition de but :* le contrôleur doit avoir un ou plusieurs objectifs (par exemple, maintenir des contraintes de sécurité dans le système) ;
- *une condition d'action :* le contrôleur doit être capable d'agir sur l'état du système dans le but de maintenir un processus au sein de limites préétablies ou de contraintes de sécurité malgré des perturbations internes et/ou externes. En présence de plusieurs contrôleurs ou décideurs, les actions doivent être coordonnées pour remplir la condition de but. Des actions non coordonnées peuvent en effet mener à des accidents lorsque les contrôleurs ne respectent pas leurs responsabilités ;

- *une condition de modèle* : le contrôleur doit posséder un modèle du système. Les accidents survenant dans les systèmes complexes résultent fréquemment d'incohérences entre le modèle du processus utilisé par le contrôleur (qu'il soit humain ou automatisé) et l'état présent du système ;
- *une condition d'observabilité :* le contrôleur doit pouvoir vérifier l'état du système grâce aux retours d'information sur l'état du processus. Les retours et les rétroactions sont utiles pour la mise à jour du modèle de processus du contrôleur.

Le contrôleur d'une installation industrielle obtient les informations relatives à l'état du processus à partir des variables mesurées (rétroactions) et les utilise pour initier une action en manipulant les variables contrôlées afin de maintenir le processus dans les limites prédéfinies malgré les perturbations sur le processus. Généralement, la maintenance à un niveau du système ouvert demande un ensemble de processus contenant un processus de communication de l'information destiné à la régulation et au contrôle du système.

L'effet d'une action de contrôle est en général décalé par rapport au processus, car la propagation du signal au sein de la boucle de contrôle et la transmission même d'une information induisent nécessairement un certain temps de latence. Ainsi, un élément peut ne pas répondre immédiatement à un signal extérieur ; le processus peut contenir des délais de réponse, nécessaires à la manipulation des variables, de sorte que les capteurs n'obtiennent les valeurs qu'après un certain laps de temps. Ces retards restreignent la vitesse et augmentent les effets des perturbations et des fluctuations non seulement au sein du processus, mais également dans sa réponse externe, imposant du même coup au contrôleur des exigences supplémentaires. Ces retards et ses interactions sont très souvent à l'origine d'accidents au sein des systèmes générant des variations et imposant par conséquent des réponses adéquates afin d'éviter toute désynchronisation du système.

Les modèles d'accident fondés sur la théorie des systèmes considèrent que les accidents résultent d'interactions entre les éléments d'un système. Contrairement aux modèles de sécurité industrielle (qui se focalisent sur des conditions non sûres), les modèles d'accident systémiques cherchent à identifier les sources de dysfonctionnement internes à l'exploitation ou à l'organisation du système, et aux causes potentielles d'accident au travers d'interactions entre éléments.

L'approche systémique voit la sécurité comme une propriété émergente survenant lorsque les éléments interagissent au sein d'un environnement. Ces propriétés émergentes — y compris la sécurité — sont contrôlées par diverses contraintes liées au comportement des éléments du système. Les accidents apparaissent lorsque des interactions entre les éléments enfreignent ces contraintes ou lors d'un manque de contraintes.

1.4. Contrôle et sécurité

La sécurité peut donc être vue comme un problème de contrôle au sein d'un système. L'accident survient lorsque le système de contrôle se révèle incapable de maintenir efficacement une défaillance, une perturbation externe ou un dysfonctionnement entre les éléments du système. Lors de l'accident de la navette *Challenger*, le joint défaillant n'a pas pu contrôler de façon appropriée le gaz propulseur [Leveson, 2003] ; lors de la perte de la sonde *Mars Polar*, le logiciel n'a pas pu contrôler la vitesse de descente de l'appareil, impuissant qu'il était à comprendre que le « bruit » provenant des rétroactions des variables mesurées indiquait que l'engin avait atteint la surface de la planète. De tels accidents, impliquant des erreurs de conception, peuvent résulter d'un ensemble de contrôles inadéquats s'accumulant tout au long du développement du système.

S'ils sont également imposés par les fonctions de management au sein des organisations, les contrôles le sont d'une façon différente. Les enquêtes consécutives aux accidents de *Challenger* et de *Columbia* [Leveson, 2003] ont pointé du doigt l'inadéquation des contrôles dans le processus de lancement et de développement du système, ainsi que des erreurs de communication. Alors que les évènements et les comportements *défaillants* reflètent la présence d'interactions défaillantes et une application inadéquate de contraintes de sécurité, le contrôle inadéquat procède quant à lui des évènements, et donc du comportement du système. Les évènements défaillants étant dus à un comportement systémique dans un contexte donné, ils résultent donc d'un contrôle inadéquat au sein du système. La structure de contrôle elle-même doit être examinée afin de déterminer pourquoi il est inadéquat de maintenir des contraintes sur un comportement sûr et pourquoi les évènements surviennent. Dans le cas de *Challenger*, le comportement non sûr de la navette s'est traduit par le déversement de combustible de propulsion chaud par un joint torique. Ce joint n'a donc pas rempli son rôle et donc sa fonction de contrôle d'étanchéité. La perte du système est survenue en raison d'un contrôle défaillant au sein de la conception du système.

Comprendre les accidents demande également d'examiner les phases de développement et d'exploitation afin de déterminer à quel moment du développement ou de l'exploitation une contrainte de sécurité n'a pas ou a été mal intégrée au sein du système.

La théorie des systèmes fournit un fondement pour l'ingénierie des systèmes, qui sont vus comme un ensemble intégré même s'il est composé d'éléments variés et spécialisés. L'objectif principal est d'intégrer les sous-systèmes au sein d'un système le plus efficace possible afin d'atteindre l'objectif global à partir d'exigences et de critères de conception définis. L'optimisation de la conception du système demande souvent de consentir à des compromis parmi ces critères de conception.

Une approche de sécurité en ingénierie des systèmes postule que certaines propriétés (émergentes) des systèmes, comme la sécurité, ne peuvent être

appréhendées dans leur globalité qu'en considérant toutes les variables ainsi que les aspects sociaux et techniques.

Par conséquent, l'optimisation d'un sous-système ou des éléments ne saurait mener à l'optimisation du système ; en fait, l'amélioration d'un sous-système peut même aggraver l'état et la performance du système en raison des interactions non linéaires entre les éléments. De plus, le comportement des éléments ne peut pas être compris si l'on ne considère pas les éléments dans leur ensemble et leurs interactions avec les autres éléments du système. Les tentatives d'amélioration de la sécurité à long terme ont souvent été synonymes d'échec[8]. C'est pourquoi tout modèle d'accident fondé sur la théorie des systèmes doit tenir compte de ces principes d'ingénierie des systèmes et de ce besoin constant de sécurité. Les modèles ne respectant pas ces principes fondamentaux se révèlent immanquablement limités dans leur capacité à maintenir un état d'équilibre et donc à prévenir les accidents, créant par conséquent un phénomène de désynchronisation entre le système et son environnement. Les modèles intégrant ces principes peuvent quant à eux améliorer leur propre capacité à développer des systèmes complexes de façon sûre.

2. Les concepts du modèle STAMP

Au sein du modèle STAMP, la sécurité est traitée comme un problème de contrôle. Ici, le contrôle ne désigne pas une stricte structure de commandement et de contrôle dans l'acception militaire ; le contrôle peut être influencé par une autorité, une politique, des procédures, des normes, une réglementation, des valeurs partagées et par tout autre aspect ou culture organisationnelle, mais également par son environnement, lui-même influencé par le contexte social et organisationnel, ou par les réglementations dans lequel le comportement apparaît. Le contrôle passe alors notamment par l'intégration de contraintes au sein d'une structure de contrôle dans le but de maintenir le système à l'intérieur de limites sûres tout en préservant une vision claire et complète des modèles de processus.

Dans ce cadre, le modèle STAMP recouvre trois concepts interreliés : les contraintes de sécurité, les structures de contrôle hiérarchiques et les modèles de processus.

8 Des pistes de réflexion sont apportées dans le chapitre 5 concernant les perspectives. Ces pistes passent notamment par l'intégration de la notion de chaos afin d'expliquer la sensibilité aux conditions initiales d'un système dynamique non linéaire et par une tentative de réponse au fait que toute prédiction dynamique de la sécurité à long terme est inefficace.

2.1. Les contraintes de sécurité

La notion de contrainte est au cœur du modèle STAMP. Dans la théorie des systèmes, le contrôle appelle toujours à l'intégration de contraintes. L'accident n'y est pas vu comme le résultat d'une suite d'évènements, mais comme une insuffisance ou un manque dans l'intégration de contraintes à chaque niveau d'un système socio-technique. Les contraintes de sécurité ciblent donc les relations et les prises de décision entre les variables du système constituant des états systémiques non dangereux. Ces contraintes sont également associées à un processus de contrôle visant à gérer le comportement du système en termes de changements et d'adaptations.

Ainsi, le rôle de l'ingénieur en sécurité est d'identifier les contraintes nécessaires au maintien d'un état de sécurité au sein du système et de s'assurer que la conception intègre ces contraintes et les aspects sociaux et organisationnels, et non uniquement des aspects techniques. Cette intégration doit être effectuée à tous les niveaux hiérarchiques du système et par l'ensemble des acteurs du système.

Les systèmes socio-techniques peuvent être lus et modélisés comme une hiérarchie de niveaux organisationnels associés à des processus de contrôle fonctionnant à l'interface entre les niveaux afin de contrôler les processus des niveaux inférieurs. À chaque niveau, un contrôle inadéquat peut provoquer l'omission, l'application incorrecte ou la transmission erronée d'une contrainte au niveau inférieur. Comme vu au chapitre 1, la modélisation des systèmes socio-techniques n'est pas nouvelle ; Jay Forrester en a été l'un des précurseurs en mettant en évidence la dynamique des systèmes, qui a notamment permis de développer au sein du modèle STAMP, la notion de structure de contrôle.

2.2. Les structures hiérarchiques de contrôle de la sécurité

La prévention ou l'analyse des accidents imposent de concevoir une structure de contrôle incluant le système socio-technique le plus représentatif possible d'un contexte ; cette structure appliquera les contraintes nécessaires au niveau du développement et lors de l'exploitation du système conformément à ses exigences fonctionnelles. Cette structure de contrôle (figure 12) peut être décrite pour chaque système.

La théorie des systèmes appréhende un système comme une structure hiérarchique dans laquelle chaque niveau impose des contraintes à l'activité du niveau inférieur [Leveson, 2004 ; Leveson, 2006]. Les accidents résultent d'une application inadéquate de contraintes au sein des niveaux du système socio-technique.

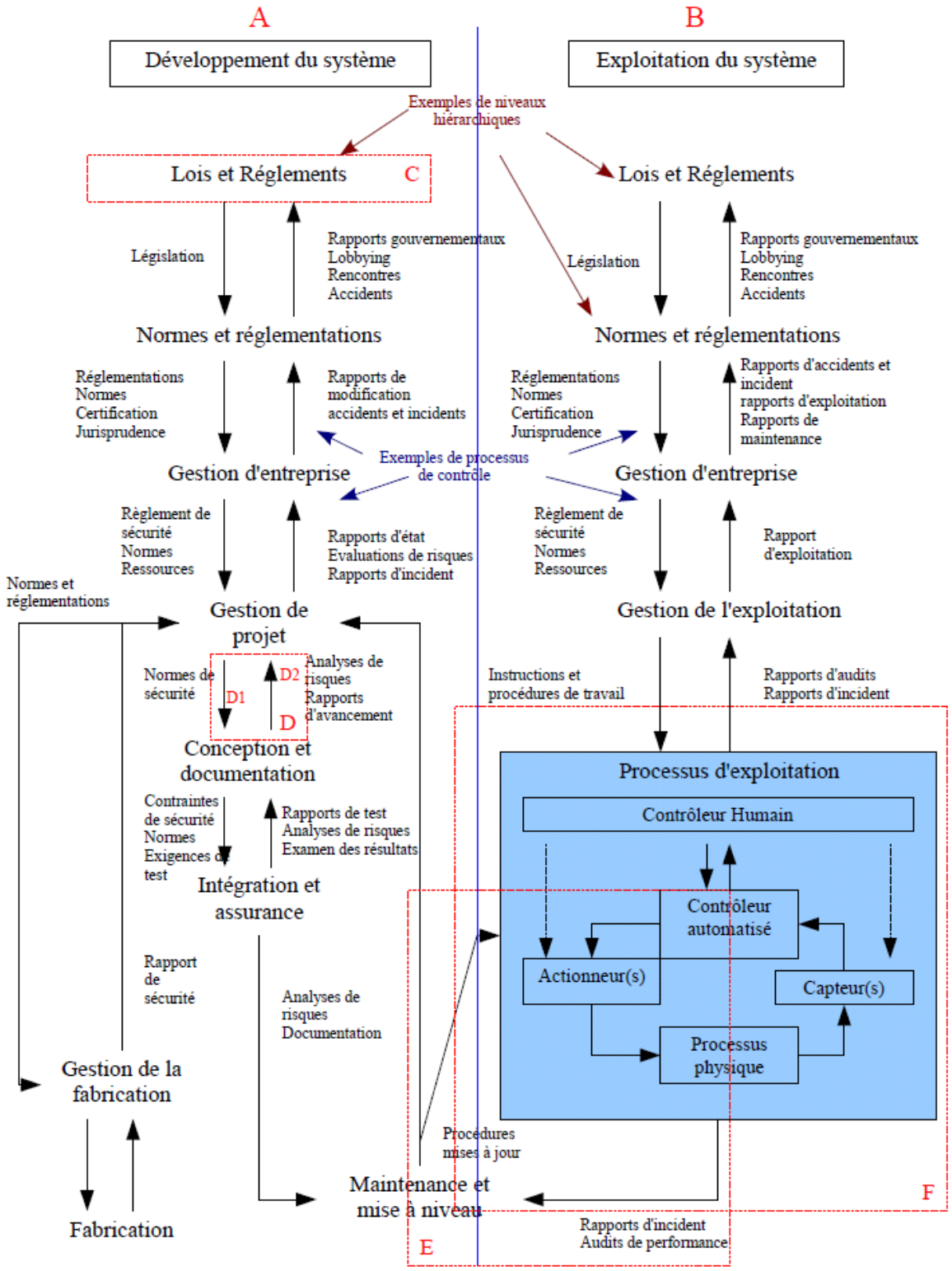


Figure 12 ■ Représentation générale d'une structure de contrôle socio-technique
adapté de Leveson [Leveson, 2005]

Modéliser des organisations complexes dans un contexte donné et dans le cadre du modèle d'accident STAMP implique d'organiser ces systèmes en niveaux hiérarchiques avec des processus de contrôle opérant entre chacun d'eux. Ce modèle général possède deux structures de contrôles hiérarchiques (A et B séparées par une barre verticale) : la structure A pour le développement du système et une structure B pour l'exploitation du système intégrant les interactions entre les différents niveaux hiérarchiques aussi bien horizontaux que verticaux (C). La sécurité durant l'exploitation du système dépend partiellement de la structure, de la conception originale et du développement ainsi que des actions de contrôle durant l'exploitation. Rappelons que la sécurité est une propriété émergente dans un système et qu'elle ne peut être améliorée qu'en adoptant une vision holistique.

Entre chaque niveau hiérarchique (D) de chaque structure de contrôle, des canaux de communication efficaces sont nécessaires. La transmission descendante de l'information — c'est-à-dire du niveau supérieur au niveau inférieur (D_1) — permet l'intégration de contraintes et l'application d'un contrôle, tandis que la transmission ascendante (D_2) permet de fournir une rétroaction concernant l'intégration satisfaisante ou non de la contrainte de sécurité. Ces échanges entre niveaux hiérarchiques permettent à chaque niveau de remplir ses responsabilités en matière de sécurité. La rétroaction est importante dans tout système ouvert afin de produire un contrôle adéquat et/ou de vérifier que ce contrôle est bien adéquat.

Dans le développement d'une structure de contrôle, les normes, les règlements et la politique de l'entreprise sont adaptés afin d'atteindre les exigences du système. Les contraintes de conception identifiées comme nécessaires au contrôle des dangers systémiques sont transmises aux développeurs et aux certificateurs en accord avec les réglementations et les exigences. La validation finale dépend des rapports de tests ainsi que des différentes analyses de dangers et de risques. À la fin du processus de développement, les résultats des analyses de risques sont rassemblés au sein de documents de conception et de développement servant au maintien du niveau de sécurité au cours du cycle de vie du système (maintenance).

Ce processus est relativement identique pour la structure de contrôle opérationnelle (B).

Par ailleurs, les structures de développement interagissent avec les structures d'exploitation. Les exigences en matière de sécurité servant à la conception et au développement d'un système constitueront les « fondements sécuritaires » des procédures opérationnelles.

Des retards dans la transmission des informations peuvent affecter le flux des actions de contrôle et de rétroaction et ainsi retentir sur la performance de la boucle de contrôle — donc sur la sécurité d'un système.

Les accidents résultent d'un défaut dans les boucles de contrôle en raison d'une application inadéquate de contraintes de sécurité sur le comportement des éléments d'un système. Ces dysfonctionnements affectant les interactions entre les niveaux

hiérarchiques d'une organisation résultent des défaillances des éléments et des défauts en conception.

Le processus accidentogène peut donc être appréhendé comme un ensemble de défauts affectant les éléments des boucles de contrôle lors du développement et de l'exploitation du système durant l'ensemble des phases et du cycle de vie du système, c'est-à-dire comme un ensemble de défauts perturbant les interactions entre les éléments du système, engendrant ainsi des prises de décision inadéquates.

Ces différents défauts peuvent être classés afin d'analyser et/ou de prévenir les accidents, et pour identifier les facteurs inclus dans un accident et leurs interactions. Ainsi, le modèle STAMP permet d'une part de prévenir et d'analyser les dangers et les risques au sein d'un système, et d'autre part de comprendre le comportement d'un système ayant pu mener à un accident ou à une perte d'équipements ou de ressources.

L'analyse des modèles de processus (le troisième socle du modèle STAMP avec les contraintes et les niveaux hiérarchiques de contrôle) jouent un rôle significatif dans cette classification des défauts.

2.3. Les modèles de processus et les boucles de contrôle

Un processus de contrôle (F) fonctionne entre chacun des niveaux de la hiérarchie décrite précédemment. Un processus de contrôle a pour objectif de traduire un entrant provenant d'un niveau hiérarchique en un contrôle sur un autre niveau hiérarchique ; ce processus peut aussi bien être descendant qu'ascendant. Il est schématisé par une boucle de contrôle qui le décrit (figure 13).

Dans cette boucle servant à comprendre l'« esprit » de la démarche, le contrôleur utilise les informations de contrôle en entrée ainsi que les différentes mesures pour générer des commandes. La commande est ensuite envoyée à un actionneur qui transforme cette commande en action à travers le vecteur U.

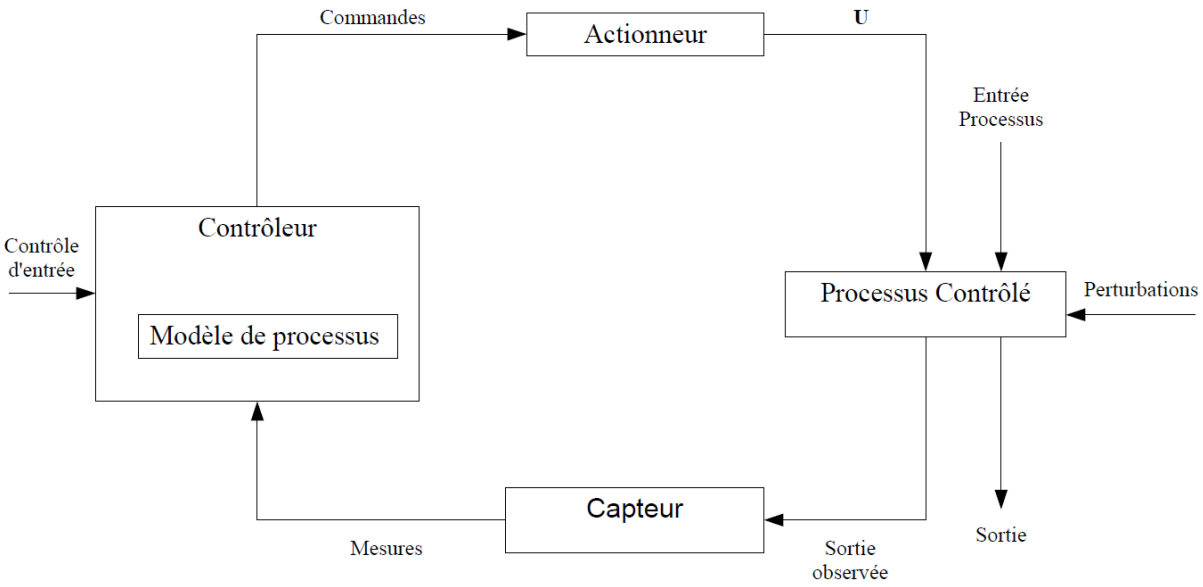


Figure 13 ■ Boucle de contrôle de processus
adapté de Leveson [Leveson, 2007]

Le vecteur U représente les actions de l'actionneur qui auront une influence sur le processus contrôlé. L'algorithme de contrôle utilisé par le contrôleur est fondé sur un processus interne de processus contrôlé. Le processus contrôlé, qui peut représenter l'installation industrielle, est soumis à des entrées de processus provenant de niveaux hiérarchiques ou de perturbations. Les résultats de processus peuvent constituer une source d'information pour un processus connexe. Les capteurs mesurent les sorties de processus résultant des actions de l'actionneur et des perturbations et génèrent de nouvelles mesures visant à alimenter l'observateur. Le contrôle d'entrée peut être tout simplement un objectif, une fonction ou un but assigné à un système. Le contrôleur peut envoyer des directives à un contrôleur de niveau inférieur plutôt qu'à un actionneur dans le but d'impacter le contrôle d'un processus.

L'intégration du modèle cognitif de l'opérateur humain dans un processus contrôlé est de première importance. De manière générale, n'importe quel contrôleur (humain ou automatisé) a besoin d'un modèle du processus afin de contrôler efficacement un système. Qu'un système soit relativement simple ou extrêmement complexe, l'ensemble des opérateurs et les contrôleurs doivent avoir intégré le modèle de processus afin de pouvoir agir au sein de ce système de façon efficace.

Si le modèle est intégré dans une logique de contrôle automatisé (figure 14) ou de contrôle par un opérateur humain (figure 15), il doit contenir le même type d'informations : les relations entre les variables du système (les lois de contrôle), l'état actuel du système (les valeurs actuelles des variables du système) ainsi que les façons dont le processus peut agir et changer l'état du système. Ce modèle est utilisé afin de définir les contrôles nécessaires et il est alimenté et mis à jour grâce à des boucles de rétroaction. Ce modèle de processus est également nécessaire à tous les niveaux hiérarchiques d'une organisation et pas uniquement au niveau le plus bas.

Dans des systèmes complexes, une ou plusieurs boucles de contrôle peuvent relier les niveaux hiérarchiques de chaque structure de contrôle, avec un canal descendant fournissant les informations et les commandes nécessaires pour imposer les contraintes au niveau inférieur, et un canal ascendant permettant de rendre compte de l'efficacité de ces contraintes. À chaque niveau de la structure de contrôle, des contrôles inadéquats peuvent résulter d'un oubli de contraintes de sécurité, d'une mauvaise communication des contraintes de sécurité ou bien de contraintes de sécurité incorrectement appliquées au niveau inférieur. C'est pourquoi les rétroactions revêtent une dimension si particulière durant l'exploitation d'un système. Par exemple, le processus d'analyse de la sécurité générant les contraintes inclut toujours des hypothèses concernant l'environnement d'exploitation du processus. Lorsque l'environnement change, rendant ces hypothèses fausses, les contrôles en place ne sont plus adéquats. Ce décalage entre l'environnement et le système peut être à l'origine d'une désynchronisation et d'un comportement inadéquat voire dangereux.

Les figures 14 et 15 montrent une boucle de contrôle opérant entre les niveaux hiérarchiques. Elles schématisent un processus de boucles de contrôle comportant un contrôleur automatisé supervisé par un contrôleur humain (figure 14) ainsi qu'un processus géré par un opérateur humain (figure 15), associés à des outils d'aide à la décision.

Ces modèles de processus doivent inclure les propriétés principales des capteurs, des actionneurs et quelques aspects de l'environnement, particulièrement lorsqu'ils peuvent être à l'origine de perturbations. Un de ces aspects est l'intégration d'une interface avec les contrôleurs humains contenant l'ensemble des contrôles, des affichages et des avertisseurs en cas de danger qui est un moyen grâce auquel les modèles de contrôleurs automatisés et humains peuvent se synchroniser. Un manque de synchronisation entre ces deux modèles contrôleurs peut être à l'origine d'accidents au sein du système en raison de délais de réponse trop importants ou d'informations incorrectement transmises.

Ces modèles de processus ne sont pas seulement essentiels lors du fonctionnement du système mais ils sont également utilisés lors du développement du système. Chaque contrôleur doit disposer d'un modèle de l'état du système devant être contrôlé, d'un modèle des interactions entre les variables du système et des modalités selon lesquelles les processus modifient l'état du système. Les accidents — notamment systémiques — résultent d'incohérences dues à des décalages entre le modèle de processus utilisé par les contrôleurs et l'état du système à un instant donné.

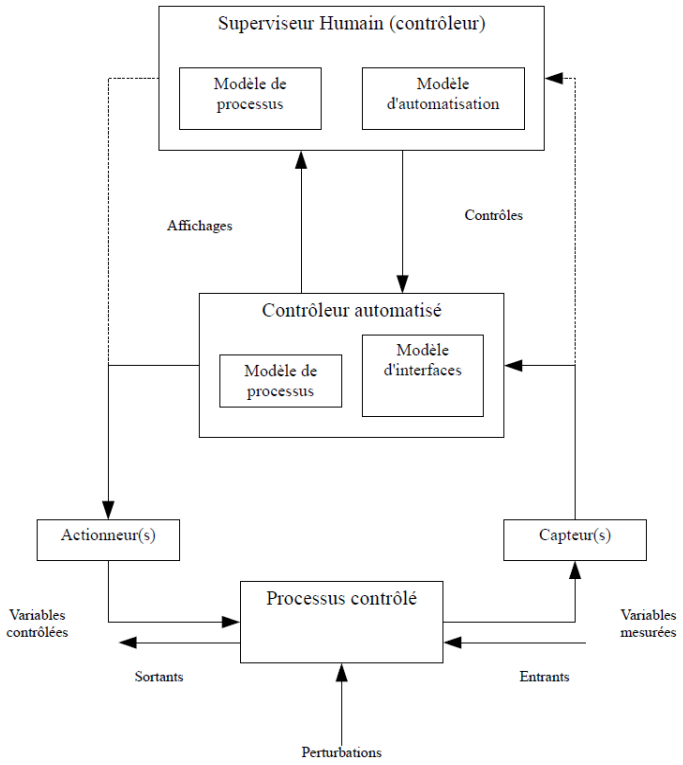


Figure 14 ■ Processus automatisé mais supervisé par un contrôleur humain
Adapté de Leveson [Leveson, 2005]

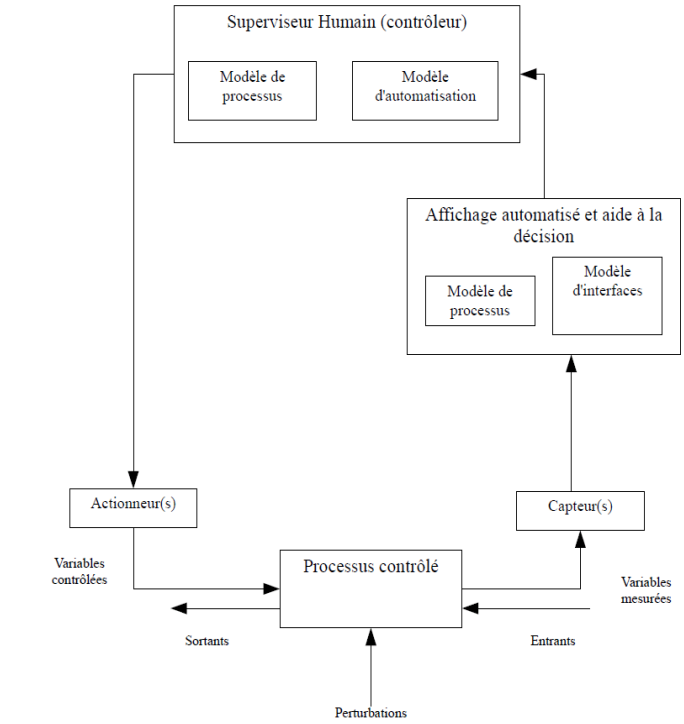


Figure ■15 ■ Processus contrôlé par opérateur humain avec une assistance automatisée
adapté de Leveson [Leveson, 2005]

Les concepteurs d'un système impliqués dans son développement et son exploitation peuvent utiliser aussi bien les modèles du système conçu que les modèles du processus de développement et d'exploitation. L'intégration de ces modèles permet une prise en charge performante des contraintes de sécurité au sein du système afin d'éviter que des situations inadéquates ne mènent à des accidents.

Dans le modèle STAMP, l'accident est défini comme le non-respect d'une contrainte de sécurité provoquant une défaillance dans les éléments du système due à une perturbation environnementale ou à un dysfonctionnement au sein des interactions entre les éléments.

Dans chaque boucle de contrôle de chaque niveau de la structure de contrôle socio-technique d'un système donné, un comportement non sûr se traduit soit par un oubli de contrainte, soit par une contrainte inadéquate sur le processus du niveau inférieur, soit encore par une application inadéquate de la contrainte (tableau 4).

Chaque élément de la boucle de contrôle associée à un processus de contrôle prend part à l'application de contraintes de sécurité ; la classification de ces contraintes débute par l'examen de chaque élément de la boucle de contrôle principale en évaluant sa participation éventuelle : le contrôleur peut débuter une action de contrôle inadéquate ou inadaptée, amenant des défaillances ou des perturbations dans le processus physique ou bien des actions de contrôle peuvent être exécutées de façon inadéquate par l'actionneur. Ces facteurs généraux s'appliquent à chaque niveau de la structure de contrôle socio-technique tout en pouvant être spécifiques d'un niveau à un autre.

1. Application non-conforme de contraintes (Actions de contrôle)
    1.1 Dangers non identifiés
    1.2 Actions de contrôle inappropriées, inefficaces ou oubliées pour un danger identifié
        1.2.1 Développement de l'algorithme de contrôle sans application de contraintes
            - Défaut dans la création du processus
            - Modifications dans le processus sans modification adéquate dans l'algorithme de contrôle
            - Modification ou adaptation incorrecte
        1.2.2 Modèles de processus incohérent, incomplet ou incorrect
            - Défaut dans la création du processus
            - Défaut dans la mise à jour du processus
            - Rétroaction inadéquate ou oubliée
                - Non incluse dans la conception du système
                - Défaut de communication
                - Délais
                - Opération du capteur inadéquate
            - Délais ou mesure imprécises
        1.2.3 Coordination inadéquate entre les contrôleurs et les décideurs
2. Execution non-conforme d'une action de contrôle
    2.1 Défaut de communication
    2.2 Opération inadéquate de l'acteur
    2.3 Délais

Tableau 4 ■ Classification des erreurs de contrôle menant à des dangers
adapté de Leveson [Leveson, 2005]

Ces trois concepts (contraintes, structures de contrôle et modèle de processus) constituent les fondements théoriques du modèle d'accident STAMP et de la technique d'analyse STPA, qui fait l'objet du paragraphe suivant.

3. L'analyse des dangers STPA fondée sur le modèle STAMP

Cette troisième section présente la technique d'analyse STPA, une analyse des dangers développée à partir du modèle d'accident STAMP. L'analyse des dangers STPA (« *STAMP-based Analysis* ») a été décrite par Nancy Leveson et son équipe [Leveson, 2003 ; Dulac, 2004 ; Daouk, 2004 ; Stringfellow, 2007]. Cette analyse se fixe deux principaux objectifs, qui sont ici successivement présentés : l'enquête accident sous les angles statique et dynamique, et l'évaluation de la sécurité.

3.1. STPA pour l'analyse d'accident[9]

L'analyse des dangers STPA est un processus itératif fondé sur le modèle d'accident STAMP permettant d'analyser les origines et les causes d'un accident. Dans STPA, le système est vu comme un ensemble de boucles de contrôle interagissant entre elles. L'accident se traduit par un contrôle inadéquat. L'objectif étant, dans une démarche d'enquête accident, de mettre en exergue les actions de contrôle constituant la cause d'une migration vers l'état accidentel.

Toute analyse d'accident STPA débute par une identification des dangers « système » afin de les traduire en contraintes de sécurité à un niveau stratégique. L'étape suivante définit la structure de contrôle de la sécurité en mettant en évidence les contrôles et rétroactions à l'œuvre au sein du système. Cette structure de contrôle de la sécurité est utilisée comme un « guide » pour effectuer l'enquête et chaque contrôle de la hiérarchie est évalué en matière d'incidence. Une identification des actions de contrôle inadéquates sert à préciser les contraintes de sécurité inadéquatement appliquées. Enfin, après avoir identifié les actions de contrôle dangereuses ayant pu mener à l'accident, des recommandations sont formulées.

Deux types de modèles, mobilisés lors de deux phases d'analyse, sont généralement nécessaires à l'étude d'un accident. Le premier est un modèle *statique* de contrôle de la sécurité permettant de visualiser l'organisation du système accident ainsi que les interactions au sein de ce système :

- les exigences et les contraintes de sécurité en place ;
- les actions de contrôles défaillantes ;
- le contexte (social, politique, économique, environnemental…) au moment de l'accident ;
- les défauts dans les modèles cognitifs des acteurs du système ;
- les défauts de coordination, de communication et d'interaction des acteurs du système.

9 Diverses analyses d'accidents utilisant le modèle d'accident STAMP ont fait l'objet de publications [Leveson, 2002 ; Leveson, Daouk, Dulac, Marais, 2003 ; Marais, 2004 ; Nelson, 2008].

Un second modèle, *dynamique* et portant sur le comportement, vise quant à lui à comprendre le comportement du système au moment de l'accident ainsi que sa migration d'un état « sûr » vers un état accidentel.

Ces modèles sont utilisés pour comprendre un accident et valider des amendements à apporter à la culture de sécurité d'un système mis à mal par l'accident. Ils peuvent être exploités pour évaluer et analyser les causes d'un accident et détecter si le niveau de sécurité a atteint un niveau inacceptable menant irrémédiablement à l'accident. Enfin, ces modèles permettent d'évaluer les impacts potentiels des changements et des décisions ayant modifié la structure d'un système, le faisant migrer vers un état accidentel.

Lors d'une enquête accident, l'analyse STPA est divisée en deux phases, l'une statique et l'autre, dynamique, dont les étapes sont reprises dans la figure 16.

3.1.1. Phase statique

La phase statique de l'analyse STPA comporte cinq étapes :

- étape 1 : analyse préliminaire des risques « système » et définition des exigences et des contraintes « système » ;
- étape 2 : établissement de la structure de contrôle de la sécurité (rôles et responsabilités des éléments et mécanismes de rétroaction) ;
- étape 3 : intégration des exigences « système » et des contraintes « système » au niveau des éléments ;
- étape 4 : examen de la structure de contrôle et des modèles de processus pour analyse détaillée des contrôles inadéquats ;
- étape 5 : catégorisation (immédiat, long terme, standard) et gestion des risques (défauts des boucles de contrôle).

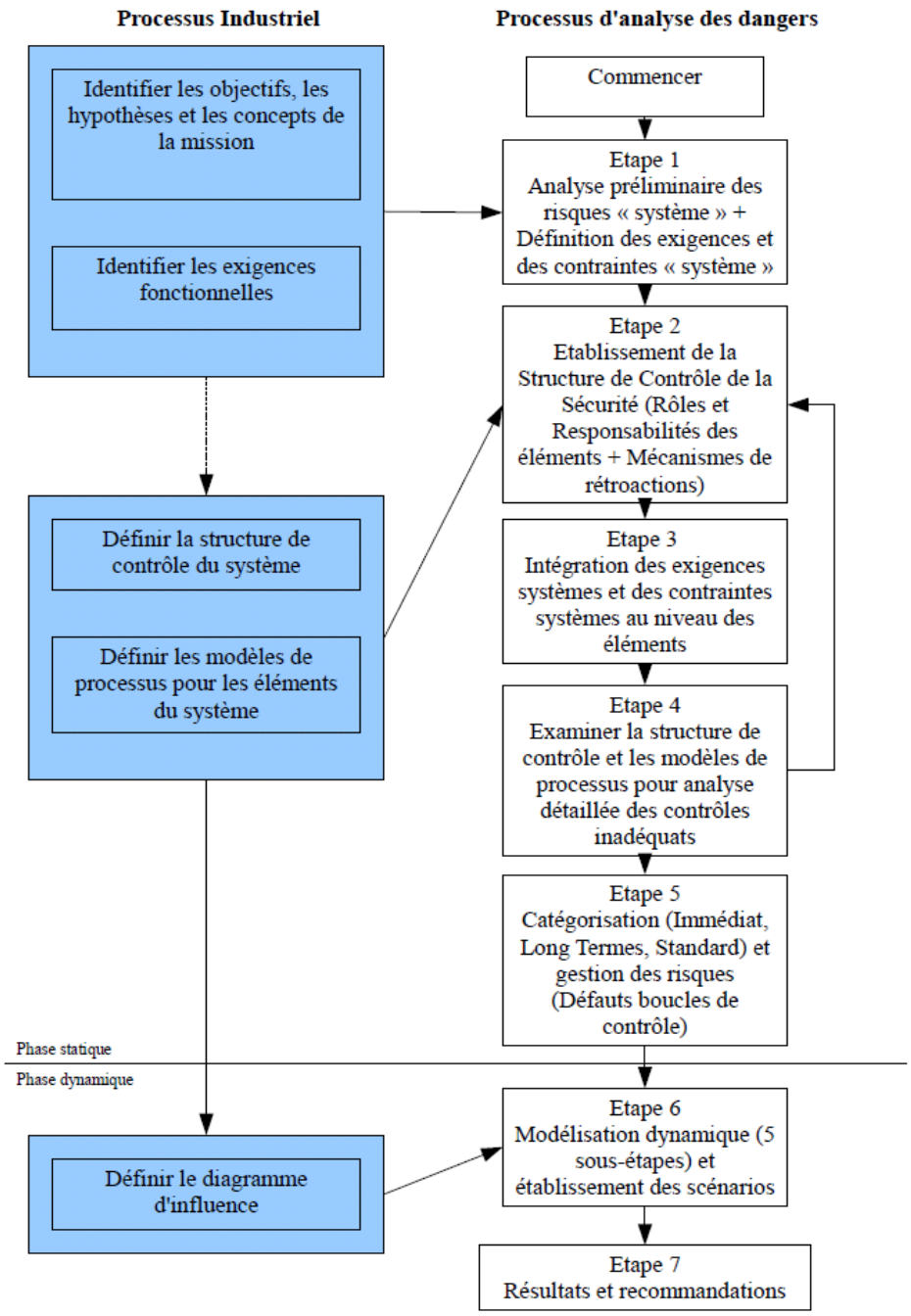


Figure 16 ■ Processus STPA en enquête accident
adapté de Leveson et Daouk [Leveson, Daouk, 2004]

► ÉTAPE 1 — ANALYSE PRÉLIMINAIRE DES RISQUES ET DÉFINITIONS DES EXIGENCES ET DES CONTRAINTES « SYSTÈME »

Cette première étape permet d'identifier les exigences globales en matière de sécurité dans le système.

OBJECTIF — Lors d'une enquête accident, une analyse préliminaire des risques et des dangers est effectuée au sein du système accident à un niveau « système » afin de définir les exigences en matière de sécurité ainsi que les contraintes en sécurité du

système. Elle permet surtout de mettre en exergue des dangers qui n'ont pas été identifiés au moment de l'accident.

MÉTHODE — Comme dans toute analyse des dangers « système », ces exigences et ces contraintes proviennent de l'examen des défaillances potentielles, des dysfonctionnements au niveau des interactions ou de conditions ne permettant pas de maintenir le contrôle du système.

Dans le cadre d'une enquête accident, un danger système reste global et concerne l'ensemble du système. À titre d'exemple, il peut être défini comme « une ingénierie et un système de prise de décision inefficaces menant à l'accident ».

À partir de ce danger, il devient possible de déterminer des exigences et des contraintes en sécurité à un niveau « système » :

- la sécurité doit être une priorité en conception et dans les processus de décision ;
- les décisions concernant les questions de sécurité doivent être traitées par des experts ;
- les analyses de sécurité doivent être disponibles et débutées le plus tôt possible dans le cycle de vie du système.

Chapman et Ward ont typologisé les différents types de dangers susceptibles d'être présents à un niveau « système » [Chapman et Ward, 2003] :

- les dangers associés aux estimations du système accident se traduisant par des exigences en termes de temps, de coûts et de qualité. Ces dangers peuvent ainsi être :
  - un manque de clarté dans la définition d'exigences de conception/développement dont le risque serait une exploitation inadéquate du système menant à l'état accidentel ;
  - un manque de maîtrise dans un domaine qui aboutirait à une action de contrôle inadéquate ;
  - la survenance d'évènements non prévus pouvant causer des pertes lors de l'exploitation du système (cf. la notion de « complexité interactive » de Perrow définie au chapitre 1, § 4.1 [Perrow, 1984])
- les dangers concernant la conception et la logistique du système accident (le processus de conception du système accident a-t-il été respecté ?) ;
- les dangers concernant les objectifs du système. Ces dangers peuvent impliquer des modifications en conception, voire des compromis importants. Il est dans ce cas important de définir des responsabilités claires et complètes pour chaque élément du système accident (*v.* Étape 2) ;
- enfin, de nombreux dangers peuvent survenir avant la survenue d'un accident en raison des interactions entre les différents éléments du système. Ces relations peuvent en effet être complexes et engendrer certains contrôles inadéquats, notamment dus :
  - à une définition incorrecte des responsabilités des éléments (*v.* Étape 2) ;
  - à une perception inadéquate du rôle et de la responsabilité des éléments ;

- à une communication inadéquate entre les éléments (*v.* Étape 4) ;
- aux fonctionnalités des éléments ;
- à une compréhension inadéquate des documents de développement et d'exploitation ;
- à des mécanismes inadéquats de coordination et de contrôle au sein du système.

► ÉTAPE 2 — ÉTABLISSEMENT DE LA STRUCTURE DE CONTRÔLE DE LA SÉCURITÉ (RÔLES ET RESPONSABILITÉS DES ÉLÉMENTS ET MÉCANISMES DE RÉTROACTION)

Cette deuxième étape permet la construction de la structure de contrôle de la sécurité suite à l'étape 1 et à l'identification des rôles et des responsabilités de chaque élément au moment de l'accident.

OBJECTIF — Cette étape permet l'établissement de la structure de contrôle de la sécurité du système accident (*v.* figure 12) incluant les rôles et les responsabilités de chaque élément aussi bien les éléments de contrôle que de rétroactions pour chacun de ces éléments au « moment » de l'accident. Cette étape permet donc *in fine* de définir et d'établir la structure de contrôle de la sécurité des systèmes telle que développée par Nancy Leveson [Leveson, 2004].

Chaque niveau ou élément de la structure de contrôle possède des rôles et des responsabilités qui permettent de s'assurer si les contraintes en sécurité des systèmes étaient appliquées ou pas. Les éléments du système à inclure ainsi définis, il est nécessaire de modéliser la structure de contrôle de la sécurité.

MÉTHODE — La première phase de la création de la structure de contrôle de la sécurité s'efforce de définir ce qu'il convient d'y inclure ou d'en exclure ; cette phase est donc proche de celle de la définition des limites d'un problème lors d'un processus de modélisation dynamique. Il est délicat d'inclure dans l'analyse les acteurs qui ont pu avoir un impact indirect sur le système. Ainsi, choisir la limite d'une analyse demande de faire certains compromis non négligeables surtout lors d'une enquête accident où le moindre élément peut avoir d'importantes conséquences. Une limite large peut améliorer la probabilité d'identification de certains facteurs ne pouvant être identifiés qu'à l'aide d'analyses supplémentaires. Les systèmes évoluent au cours du temps et les éléments à inclure ou non dans une analyse peuvent être modifiés car des changements structurels sont susceptibles d'avoir un impact important dans la dynamique d'un système. La structure impacte le comportement, qui lui-même provoque des changements structurels et peut mener à des interprétations différentes. Le modèle ainsi que les analyses doivent faire partie d'un cycle identique à celui d'un processus en sécurité des systèmes dans lequel les dangers et les analyses doivent être revus, mis à jour et précisés tout au long de l'enquête accident.

Dulac définit une liste non exhaustive, destinée à faciliter la caractérisation et l'établissement d'une structure de contrôle de la sécurité et à permettre dans un

second temps la construction d'un modèle dynamique du système (tableau 5) [Dulac, 2007].

Développement du système	Exploitation du système
Lois et règlements	Lois et règlements
Agences nationales et gouvernementales	Agences nationales et gouvernementales
Associations industrielles	Associations industrielles
Associations de consommateurs	Associations de consommateurs
Compagnies d'assurance	Compagnies d'assurance
Gestion d'entreprise	Gestion d'entreprise
Gestion de projet	Gestion d'exploitation
Ingénierie de développement	Ingénierie d'exploitation
Analyste sécurité en développement	Spécialiste risques professionnels
Mise à niveau du système	Maintenance du système
Assurance (qualité, sécurité, etc.)	Assurance d'exploitation (qualité, sécurité, etc.)
Fabrication	Fournisseur(s)
Contractant(s)	Contractant(s)

Tableau 5 ■ Liste des éléments pour une structure de contrôle
adapté de Dulac [Dulac, 2007]

Il est bon de préciser les entrées et les sorties, les rôles et les responsabilités de chacun, les actions de contrôle potentiellement inadéquates et les exigences de rétroactions. Il est également intéressant d'ajouter les facteurs environnementaux et les différents contrôles en place. Lors de cette étape, il est essentiel de mettre en évidence les différentes responsabilités et d'identifier les oublis et les conflits de responsabilités. L'ajout de responsabilités peut venir compléter une enquête accident montrant un manque dans la définition d'exigences fonctionnelles de certains éléments. Cette étape peut s'appuyer soit sur une conception organisationnelle si elle existe, soit sur une nouvelle conception qui satisfait aux exigences et aux contraintes du système. Cette structure de contrôle prend en compte les rôles et les responsabilités de chaque élément et autorise ainsi une compréhension de la structure avant et pendant l'accident.

► ÉTAPE 3 — INTÉGRATION DES EXIGENCES « SYSTÈME » ET DES CONTRAINTES « SYSTÈME » AU NIVEAU DES ÉLÉMENTS

Cette étape consiste en l'intégration des exigences identifiées lors de l'étape 1 au sein de chaque élément de la structure de contrôle.

OBJECTIF — L'intégration des exigences et des contraintes système définies lors de l'étape 1 doit s'effectuer au niveau de chaque élément de la structure de contrôle de la sécurité définie lors de l'étape 2.

MÉTHODE — Cette étape prend en compte chacun des éléments de la structure de contrôle de la sécurité et définit pour chacun d'eux des contraintes de sécurité conformes à celles définies lors de l'étape 1, tout en intégrant d'éventuelles interactions. Ces exigences et ces contraintes correspondent aux responsabilités en matière de sécurité pour chaque élément du système accident.

Exigence et contrainte de sécurité « système accident»

« Les dernières « normes et réglementations » en matière de sécurité doivent être appliquées au niveau du système afin de préserver la sécurité des employés se trouvant au niveau de la gestion de l'entreprise ».

► ÉTAPE 4 — EXAMEN DE LA STRUCTURE DE CONTRÔLE ET LES MODÈLES DE PROCESSUS POUR UNE ANALYSE DÉTAILLÉE DES CONTRÔLES INADÉQUATS

La quatrième étape est un examen de la structure de contrôle afin d'identifier les contrôles inadéquats ayant peu mené à l'accident.

OBJECTIF — Une analyse détaillée des contrôles inadéquats est requise lors de cette étape. Elle permet de définir les contrôles inadéquats ayant pu jouer un rôle dans la survenance de l'accident.

Pour ce faire, il est possible de distinguer quatre types suivants de contrôles inadéquats :

- une action de contrôle n'a pas été exécutée ;
- une action de contrôle incorrecte ou non sûre a été exécutée menant à une perte ;
- une action de contrôle potentiellement correcte a été effectuée trop tôt, trop tard, ou à un mauvais moment ;
- une action de contrôle correcte a été stoppée trop tôt.

MÉTHODE — À partir de la structure de contrôle construite lors de l'étape 2 et des responsabilités ainsi que des mécanismes de rétroaction identifiés lors de l'étape 3, les contrôles inadéquats peuvent être définis. Le but est de formuler pour chaque niveau hiérarchique les actions de contrôle inadéquates. Ces différentes actions constituent une source fondamentale dans la compréhension des causes d'un accident.

Exemple appliqué à la figure 12

Le niveau hiérarchique « gestion de l'entreprise » ne fournit pas de normes de sécurité au niveau inférieur. Ce contrôle inadéquat peut être caractéristique d'un manque de communication entre niveaux hiérarchiques.

► ÉTAPE 5 — CATÉGORISATION (IMMÉDIAT, LONG TERME, STANDARD) ET GESTION DES RISQUES (DÉFAUTS DE BOUCLES DE CONTRÔLE)

Il s'agit ici de catégoriser les risques et d'aboutir à les classer selon leur impact sur le système, en cherchant à déterminer à quel endroit d'une boucle de contrôle ces risques ont pu jouer un rôle.

OBJECTIF — Une première catégorisation des risques identifiés est d'abord effectuée afin de déterminer l'incidence d'actions de contrôle inadéquates sur le comportement du système ayant pu mener à l'accident. Puis, les défauts de contrôle sont traités en déterminant les processus ayant mené à la violation d'une ou de plusieurs contraintes de sécurité se traduisant par l'accident.

MÉTHODE — Il s'agit de classer les actions de contrôle ayant pu avoir un rôle dans la migration du système vers l'accident. On distingue trois types de risques :

- les risques à gestion immédiate : ces risques caractérisent des dangers ayant un impact immédiat sur le niveau de sécurité du système ;
- les risques à gestion à long terme : ces risques caractérisent des dangers pouvant être traités sur du long terme et ne demandant pas une gestion immédiate ;
- les risques à gestion standard : ces risques caractérisent des dangers ne demandant pas une gestion particulière ou urgente.

À partir d'une boucle de contrôle, les processus de contrôle ayant mené à l'accident peuvent être analysés (*v.* figure 14). En effet, les accidents résultant d'une action de contrôle inadéquate, le processus menant à l'accident peut être interprété comme la présence de défauts lors du développement et de l'exploitation du système. Ces défauts se trouvent dans les boucles de contrôle (figure 17) se situant entre les niveaux hiérarchiques et se traduisent par une omission ou par l'application de contraintes inadéquates menant à la violation d'un comportement sûr. L'objectif étant d'intégrer au sein du processus de contrôle les actions de contrôle inadéquates ayant pu être à l'origine d'une migration vers un état accidentel. Ainsi, en plus des actions de contraintes définies lors de l'étape 4, l'analyse de la boucle de contrôle et des modèles de processus met en évidence l'impact de ces actions sur le comportement même du niveau hiérarchique dont les conséquences se répercutent sur les autres niveaux (ascendants et descendants).

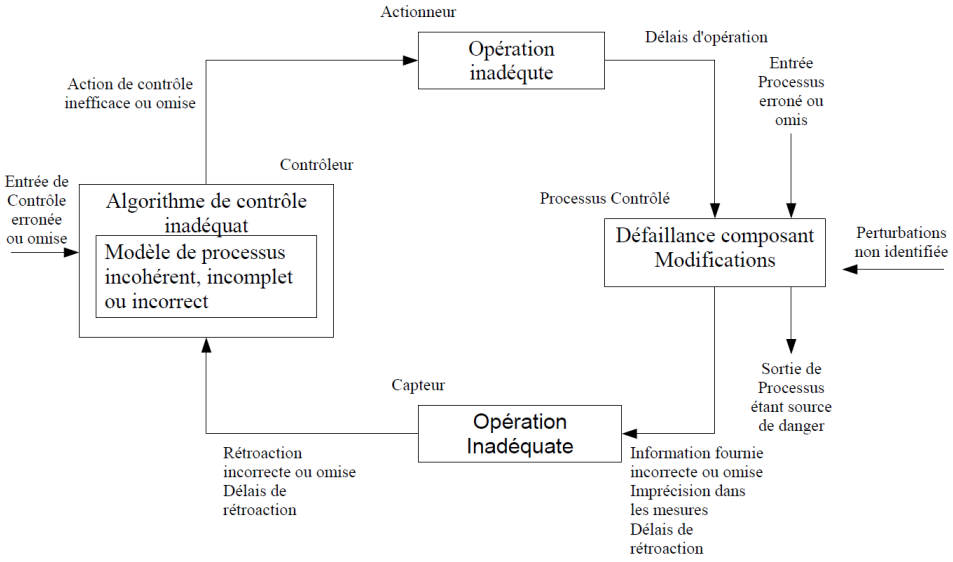


Figure 17 ■ Boucle de contrôles inadéquats
adapté de Leveson [Leveson, 2010]

La phase statique vise donc à déterminer les actions de contrôle inadéquates et les défauts de contrôle au sein des processus qui ont pu mener le système à l'accident. Cette détermination, qu'elle se fasse au niveau des interactions entre niveaux hiérarchiques (étape 4) ou au sein des processus de contrôle (étape 5) va permettre de définir des scénarios potentiels expliquant l'évolution du système jusqu'à l'accident (phase dynamique).

3.1.2. Phase dynamique

Cette phase dynamique comporte deux étapes : l'une de modélisation dynamique du système (étape 6), l'autre de formulation des résultats et des recommandations (étape 7).

► ÉTAPE 6 — MODÉLISATION DYNAMIQUE

L'étape de modélisation dynamique vise à identifier les influences entre les éléments et à mieux comprendre pourquoi et comment l'accident a pu avoir lieu.

OBJECTIF — La création et l'utilisation d'un modèle dynamique ont pour objet d'identifier les indicateurs de risque afin d'établir de nouveaux types d'analyses. Cette étape est essentielle dans une démarche d'enquête et d'analyse d'un accident. Elle permet, grâce aux outils informatiques[10], de simuler des comportements et des scénarios afin de déterminer les causes et les variables ayant pu jouer un rôle clé dans la survenance d'un accident.

10 Parmi ces outils, il est par exemple possible de citer Vensim PLE (http://www.vensim.com) ou Stella (http://www.iseesystems.com/softwares/Education/StellaSoftware.aspx).

À partir du modèle statique précédemment effectué et de la structure de contrôle de la sécurité (*v.* Étape 2), cette étape consiste à créer un modèle dynamique au moment de l'accident, qui permet d'identifier les comportements dynamiques responsables de la migration du système vers un état dangereux ou à haut risque.

MÉTHODE — La construction de ce modèle dynamique reste conforme au cycle de construction de modèle dynamique de John Sterman [Sterman, 2000]. Le processus de modélisation dynamique proposé ici est adapté des travaux de Sterman dans le domaine de la dynamique des systèmes (tableau 6).

Le modèle dynamique est précisé et complété à chaque nouvelle information provenant des éléments en interaction. Sa validation est un processus continu et itératif.

Trois types d'informations sont habituellement utilisés afin de créer un modèle dynamique [Forrester, 1992] : les données numériques, les sources textuelles et les modèles cognitifs des concepteurs inclus dans le processus de modélisation. Parmi ces trois types, Forrester précise que les modèles cognitifs sont la source la plus importante d'information.

La création d'un modèle dynamique passe donc par cinq paliers (tableau 6). Le premier consiste à définir le système accident en exploitant la structure de contrôle définie lors de l'étape 2 de la phase statique. Cette étape permet de définir les différents paramètres de « base » du système comme son temps de vie, l'unité des variables… Elle permet également de définir le couplage entre les éléments du système [Perrow, 1999] et de connaître l'incidence de certains changements sur d'autres parties du système. Une autre notion définie par Perrow doit être prise en compte dans le processus de modélisation dynamique : la complexité interactive (c'est-à-dire la présence d'évènements « non prévus » dans un système), qui influence l'occurrence voire les conséquences d'accidents majeurs au sein des systèmes complexes (*v.* Étape 1). Ces évènements non prévus peuvent se traduire par des boucles de rétroaction contenant des actions de contrôle inadéquates. Il est également nécessaire de prendre en considération la gravité des accidents ainsi que le temps de « retour à la normale » (délai) après un accident ou une perte qui peuvent influencer la dynamique du système. Dans ce cadre, la prise en compte des informations de la phase statique est également une part importante de la caractérisation du système, tout comme l'incertitude dans les prises de décisions politiques ou stratégiques.

Définition du système accident
■ Quel est l'accident ? Pourquoi est-ce un accident ?
■ Quelles sont les variables impliqués dans l'accident ?
■ Sur quelle échelle de temps étudier l'accident ?
■ Quel a été le comportement du système au moment de l'accident ?

Établir les hypothèses dynamiques de l'accident (évolution)
■ Quelles sont actuellement les théories sur l'évolution de l'accident ?
■ Formuler une hypothèse dynamique expliquant l'évolution du système vers l'accident par le jeu des rétroactions

Établir un modèle dynamique
■ Caractéristiques de la structure de l'accident et des règles de décisions
■ Estimation des paramètres, des relations comportementales et des conditions initiales
■ Tester pour vérifier la cohérence avec l'objectif et les limites de l'accident

Tester
■ Comparer avec l'état de référence
■ La robustesse aux conditions extrêmes
■ Tout test utile

Concevoir une stratégie de changement
■ Quelles conditions environnementales peuvent apparaître ?
■ Quelles nouvelles règles, stratégies, structures peuvent être intégrées dans le monde réel ?
■ Quels sont les effets d'une nouvelle politique ?

Tableau 6 ■ Les étapes du processus de modélisation
adapté de Sterman [Sterman, 2000]

Le deuxième palier permet de définir les hypothèses dynamiques de l'accident. Ces hypothèses ont pour but de décrire les évolutions potentielles du système jusqu'à l'accident par le jeu des rétroactions à partir de la structure de contrôle de la sécurité.

Cette structure statique « dynamisée » permet d'atteindre la troisième étape, qui est l'élaboration de la structure du modèle dynamique de la sécurité. Ce modèle dynamique ainsi complété, il est nécessaire d'y ajouter les différentes pressions, perturbations et influences extérieures à partir notamment des informations issues de la structure de contrôle de la sécurité. Ces pressions et influences peuvent notamment concerner :

- la production, les délais ;
- l'intégration de normes de sécurité et de réglementations ;
- le renforcement de la sécurité ;
- une pression sur les ressources en personnel et moyens ;
- les rapports d'incident et d'accident ;
- les rapports de performance ;

- les rapports de coûts.

Une quatrième phase, de test, permet ensuite de valider ou non le comportement des éléments au sein du système et ce, aux limites de fonctionnement du système. Ce test aux limites est réalisé la plupart du temps grâce à une boucle « aux limites » permettant d'éprouver la sécurité au sein du système en fonction du contexte. L'objectif de ce type de test est de s'assurer que la réponse des éléments d'un système socio-technique à des accidents majeurs est en cohérence avec le comportement des décideurs dans un contexte donné ; il permet également de mettre en lumière les éléments potentiellement déclencheurs d'une migration vers un état accidentel.

Ces différentes étapes ont notamment pour objectif ultime d'améliorer le modèle cognitif des décideurs afin qu'ils conservent à l'esprit un certain seuil de sécurité à ne pas dépasser. Plus généralement, l'objectif principal est ici la conception et l'exploitation d'un système au regard des conditions d'un accident afin de mettre en évidence le processus de migration et d'érosion de la sécurité ayant mené à l'accident. Dans certains systèmes et situations, il n'est pas possible de prévenir complètement l'augmentation des risques dès le départ. En fait, beaucoup de risques identifiés durant une analyse se focalisant sur les facteurs organisationnels peuvent être éliminés du système. Cette cinquième phase alimente également la demande en retour d'expérience.

► ÉTAPE 7 — RÉSULTATS ET RECOMMANDATIONS

Cette dernière étape de la phase dynamique est essentielle dans une démarche de retour d'expérience ; elle permet d'établir des propositions et d'initier des changements au sein du système « accidenté ».

OBJECTIF — Cette dernière étape du processus STPA d'analyse accident permet de présenter les résultats de l'enquête et de formuler des recommandations visant à établir une politique de changement au sein du système accidenté. Elle se traduit par une démarche de retour d'expérience dans le but d'intégrer des changements au sein des documents opérationnels afin de redéfinir les rôles et les responsabilités de l'ensemble des éléments impliqués dans un accident.

MÉTHODE — L'objectif ici étant de définir de nouvelles procédures organisationnelles, visant à modifier la structure et donc les comportements au sein du système accidenté.

La phase dynamique a donc permis de reconstituer les comportements du système accident lors de l'accident en définissant une hypothèse dynamique exploitée au sein d'un modèle dynamique. Cette phase permet ainsi de « retracer » l'évolution du système jusqu'à l'accident et de mettre en évidence les éléments qui ont joué un rôle plus important par rapport à d'autres dans la survenance de l'état accidentel.

3.2. L'analyse des dangers STPA pour l'évaluation de la sécurité

L'analyse STPA peut aussi être utilisée dans une démarche de prévention des accidents et d'évaluation du niveau de sécurité d'un système ainsi que pour collecter de l'information destinée à alimenter une conception et un développement orientés vers la sécurité. Une analyse des dangers est essentiellement une démarche visant la prévention des accidents avant qu'ils ne surviennent. Une démarche proactive de prévention des accidents, fondée sur le modèle STAMP, peut fournir l'information nécessaire à la prévention des risques et donc des accidents.

Les techniques actuelles d'analyse des dangers, telles que celles rencontrées en sûreté de fonctionnement par exemple, ne sont pas assez efficaces pour prendre en considération l'aspect dynamique des systèmes modernes et les systèmes complexes dans lesquels les interactions homme-machine sont importantes.

Les objectifs de l'analyse des dangers STPA sont relativement semblables à ceux d'une analyse des dangers traditionnelle :

- elle vise d'une part à identifier les dangers tout au long du cycle de vie d'un système ainsi que les contraintes de sécurité associées afin de maintenir un niveau de sécurité acceptable ;
- d'autre part, elle vise à déterminer comment ces contraintes de sécurité peuvent être violées et comment ces contraintes peuvent mener à des actions inadéquates poussant le système vers un état accidentel.

La démarche de l'analyse STPA pour une évaluation de la sécurité d'un système est fondamentalement identique à celle pour l'analyse d'accident, à quelques nuances près (figure 18).

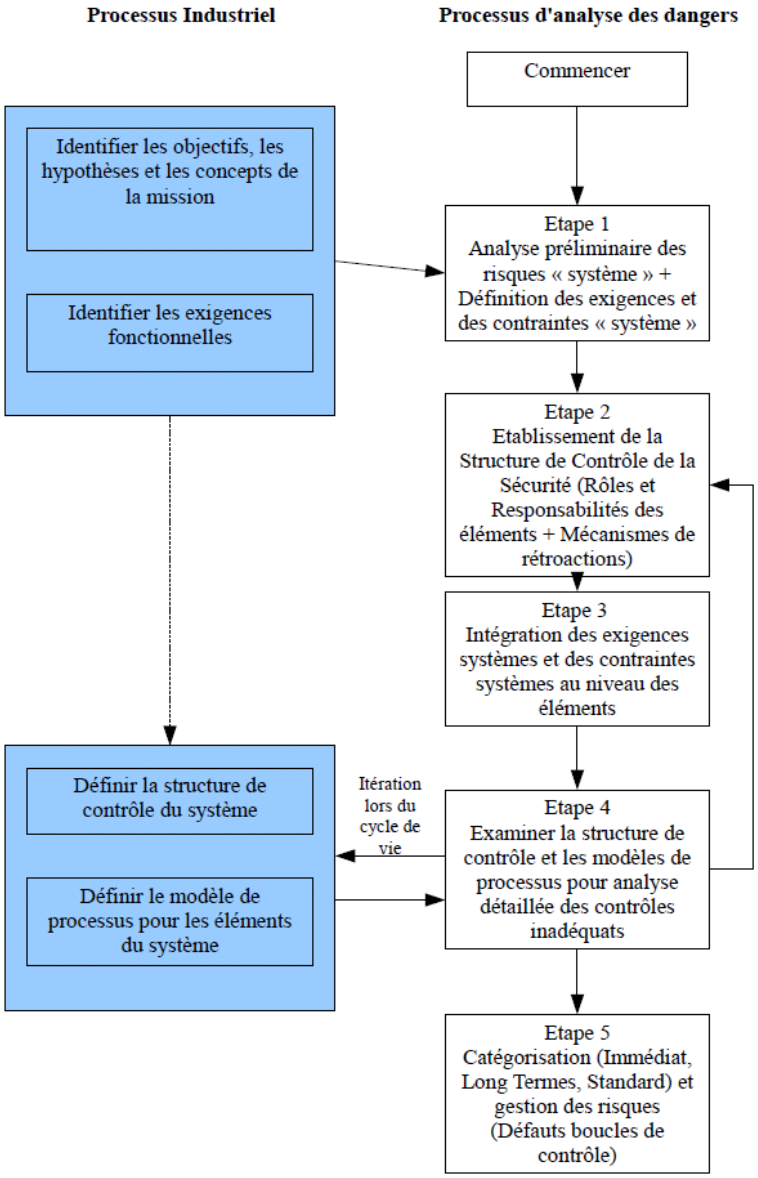


Figure 18 ■ Processus STPA en évaluation de la sécurité
adapté de Leveson et Daouk [Leveson, Daouk, 2004]

Comparativement au processus de l'analyse des dangers STPA dans le cadre d'une enquête accident, le processus d'évaluation de la sécurité laisse une place moins importante au modèle dynamique et aux simulations dynamiques. En effet, l'analyse STPA se place dans un système socio-technique dans lequel les facteurs humain et organisationnel occupent une place non négligeable. Cette présence du facteur humain implique également une incertitude comportementale ainsi qu'un manque d'information. Cette incertitude implique par conséquent un travail supplémentaire dans la recherche de l'information, visant à l'intégrer à la modélisation dynamique. Malgré cette difficulté, l'analyse STPA ne se cantonne pas au facteur technique lors d'une analyse, mais prend en compte les facteurs humain et organisationnel.

L'analyse STPA débute dès les premières étapes du développement d'un système et se poursuit tout au long de son cycle de vie [Ishimatsu, 2010]. Son utilisation durant la conception permet l'intégration d'un processus de conception sûr dans lequel l'analyse des dangers influence les décisions de conception et sont ainsi précisées et complétées lorsque de nouvelles informations sont disponibles.

L'analyse STPA possède des objectifs similaires à toutes les autres méthodes d'analyse de dangers : l'identification des dangers du système et des contraintes de sécurité afin de garantir un niveau de sécurité acceptable et une collecte d'informations à propos de ces dangers, permettant de les éliminer, de les réduire ou de les contrôler. L'analyse STPA est fondée sur le modèle STAMP et prend en compte les aspects logiciels et matériels, les processus de décision et les facteurs organisationnels dans les accidents. L'analyse STPA conserve l'imprégnation de sa filiation avec la théorie du contrôle, et se polarise par conséquent davantage sur le contrôle des dangers plutôt que sur l'élimination des défaillances des éléments, qui ne constituent qu'un seul type de causes de danger.

L'analyse STPA est utilisée pour identifier les contraintes de sécurité devant être appliquées ultérieurement ainsi que le contrôle requis pour appliquer ces contraintes et les raisons expliquant que ce contrôle puisse éventuellement être inadéquat. Ces informations étayent la prise de décision à chaque étape du processus de conception, dès les premières phases du cycle de vie du système. Le processus STPA est complété à mesure que la conception progresse. Les exigences en matière de contrôle ne peuvent être totalement remplies lors de la conception ; elles servent néanmoins de références pour la performance et la conception des exigences en sécurité lors des opérations.

L'analyse des dangers STPA présente la particularité d'être dynamique, notamment grâce à son processus itératif qui permet de prendre en compte toute information susceptible d'intéresser l'analyste dans sa démarche de prévention. Cet aspect dynamique vise à maintenir une synchronisation entre le système et l'état réel, qui se traduit par une mise en phase du système avec son environnement afin d'éviter toute migration vers un état accidentel. À l'inverse des techniques d'analyse traditionnelles, typiquement statiques et se focalisant sur la capacité du système à éviter les états instables au regard d'une conception actuelle d'un système et de son environnement, la technique STPA admet que les systèmes sont par nature dynamiques et qu'ils s'adaptent et évoluent tout au long de leur cycle de vie.

Plus concrètement, l'analyse des dangers STPA repose sur le principe d'une boucle de processus de contrôle.

Une analyse complète des dangers doit identifier les changements possibles au cours du temps dans les contrôles de sécurité pouvant conduire à des états non sûrs, voire accidentels. Des diagrammes d'influence peuvent alors être utilisés. L'information issue de l'analyse peut être exploitée pour prévenir des changements lors de la conception du système ou, dans le cas contraire, générer des mesures ou

des procédures afin de détecter des dégradations ou concevoir des contrôles lors de la maintenance ou lors de ces changements.

Le processus d'analyse des dangers STPA est divisé en cinq étapes (*v.* figure 18), méthodologiquement semblables aux étapes de l'analyse accident :

- étape 1 : analyse préliminaire des risques « système » et définition des exigences et des contraintes « système » ;
- étape 2 : établissement de la structure de contrôle de la sécurité (rôles et responsabilités des éléments et mécanismes de rétroactions) ;
- étape 3 : intégration des exigences « système » et des contraintes « système » au niveau des éléments ;
- étape 4 : examen de la structure de contrôle et des modèles de processus pour analyse détaillée des contrôles inadéquats ;
- étape 5 : catégorisation (immédiat, long terme, standard) et gestion des risques (défauts de boucles de contrôle).

En résumé, la technique d'analyse des dangers STPA doit être appliquée de façon à la fois itérative et opportuniste. Les ingénieurs pourront soit appliquer une technique particulière, soit appliquer STPA pour couvrir un ensemble de dangers plus important. Dès les premières phases de conception, certaines décisions peuvent être prises mais des défauts de contrôle ou des exécutions de contrôle inadéquates peuvent ne pas être encore identifiables. Cependant, l'analyse des dangers STPA, appliquée précocement dans le cycle de vie d'un système, permet de fournir des informations au processus de conception sur l'état du système et de son niveau de risque.

La taxonomie (*v.* tableau 4) de STPA est utilisée pour identifier les contrôles inadéquats pouvant mener à des actions de contrôle inadéquates. À partir d'elle, les ingénieurs peuvent créer de nouvelles contraintes de sécurité, compléter une contrainte existante ou créer une nouvelle conception jusqu'à ce que les dangers soient gérés, éliminés ou contrôlés. Une conception est jugée sûre ou assez sûre dès que le niveau de contrôle de la sécurité peut être considéré comme acceptable.

Conclusion

Ce chapitre a eu pour objectif de présenter et de décrire le modèle STAMP développé par le Professeur Nancy Leveson. D'un point de vue théorique, ce modèle est fondé sur la théorie des systèmes (*v.* chapitre 2) et sur la théorie du contrôle, qui a fait l'objet du début du présent chapitre, notamment dans ses applications en sécurité des systèmes. Les boucles de contrôle ont été présentées comme processus permettant de traduire une entrée en un contrôle entre chaque niveau hiérarchique.

Ont ensuite été décrits les pierres angulaires du modèle STAMP : la contrainte, la structure de contrôle et le modèle de processus.

Une troisième section a présenté un outil dérivé du modèle d'accident STAMP, appelé STPA, développé à partir des concepts du modèle STAMP et permettant l'opérationnalisation de ce modèle au sein de systèmes, pour effectuer une démarche d'enquête accident ou évaluer le niveau de sécurité d'un système tout en prenant en compte l'aspect dynamique de son comportement.

Le modèle et l'outil qui viennent d'être présentés ont été par la suite utilisés dans un système socio-technique de dépollution de sédiments contaminés, à l'état de prototype, objet du chapitre suivant.

2e partie

Résultats, limites et perspectives

Chapitre 4
Application du modèle d'accident STAMP à l'analyse des risques d'un procédé de traitement de sédiments contaminés

Ce chapitre a pour objectif de décrire l'application du modèle d'accident STAMP et l'intégration méthodologique de la technique d'analyse STPA à un système socio-technique spécifique — ici, le traitement de sédiments contaminés, système intégrant un procédé physico-chimique appelé Novosol®.

Ce chapitre est divisé en trois sections. La première section permet de décrire le contexte industriel dans lequel est appliquée la technique STPA ; elle décrit la problématique des sédiments contaminés et les différents moyens de traitement connus et employés à ce jour. La deuxième section présente un double niveau de description et d'analyse : le premier est centré sur le *procédé* technique de traitement de sédiments contaminés appelé Novosol®, tandis que le second est polarisé sur le *système* socio-technique Novosol®, mettant ainsi en évidence les interactions entre les différents contrôleurs du système. La troisième section reprend la méthode d'analyse des dangers STPA présentée dans le chapitre 3 et l'applique rigoureusement au système Novosol®. Chacune des étapes de la méthode est ainsi illustrée par les résultats issus de l'analyse.

1. Le contexte industriel d'application de la méthode STPA

Cette section présente le contexte industriel dans lequel est appliquée la technique STPA.

1.1. La problématique des sédiments contaminés

Le milieu naturel est soumis à de nombreux rejets industriels, urbains ou agricoles à l'origine d'une contamination variée et riche en polluants. En règle générale, ces contaminants restent en suspension et intègrent les vases lors de la sédimentation et sont alors immobilisés, ne présentant alors pas de réels dangers. Cependant, lorsque les conditions physico-chimiques d'un sédiment contenant des contaminants sont modifiées, ce dernier peut devenir toxique pour l'environnement ou la santé. L'exemple le plus répandu concerne les métaux lourds qui entrent dans la composition naturelle des roches mais dont la répartition a été fortement modifiée, depuis le début de l'ère industrielle, au point que l'on observe parfois aujourd'hui des concentrations multipliées par cent ou mille.

Les dégâts engendrés par les sédiments contaminés occasionnent un réel coût environnemental, social et économique. Ils sont la source de pertes importantes de revenus dues à la diminution et à la contamination d'espèces animales et végétales, mais sont aussi à l'origine de problèmes sanitaires pour les écosystèmes et les populations vivant à proximité. Les sédiments peuvent engendrer des besoins de curage car ils augmentent le risque d'inondation dans certaines zones ou diminuent le tirant d'eau de certains cours d'eau navigables.

Les principaux contaminants (cadmium, cuivre, chrome, plomb, zinc, polychlorobiphényles (PCB), hydrocarbures aromatiques polycycliques (HAP) ou arsenic) proviennent de l'activité industrielle. Ils peuvent occasionner des contaminations très variables d'un sédiment à un autre et les effets sanitaires sur des populations aussi bien végétales qu'animales peuvent s'avérer dramatiques.

Ces contaminations proviennent de diverses sources industrielles (tableau 7) pouvant générer de nombreux effets sanitaires et biologiques (dommages génétiques ou écophysiologiques, modification du comportement des espèces…)

Ce paragraphe présente la démarche de gestion des sédiments contaminés, puis les différentes techniques de traitement des sédiments contaminés.

Type d'industries	Cadmium	Cuivre	Chrome	Plomb	Zinc	PCB
Acier/fer				●	●	●
Aluminium	●		●			
Peinture anti-fouling		●		●		
Appareils électriques	●	●		●	●	●
Automobile	●	●	●		●	●
Batteries				●		
Caoutchouc					●	
Chantiers navals	●	●	●		●	●
Chimie	●		●			
Cuir/tannerie			●			
Détergents/agents de surface					●	

Distribution d'eau, gaz et électricité					•	
Explosifs		•				
Extraction de minerais précieux				•	•	
Fabrication d'oxyde		•	•		•	
Finition du métal	•	•	•	•	•	
Force motrice vapeur	•	•	•	•		
Galvanoplastie		•	•	•	•	
Munitions		•			•	
Photographie			•			
Pigments/Encres				•		
Planches d'impression					•	
Plastiques				•		
Processus métallurgiques					•	
Raffinerie du pétrole				•		
Sources non ponctuelles	•	•	•	•	•	
Traitement des eaux usées		•	•	•	•	•

Tableau 7 ■ Sources de contamination des sédiments
Source : Commission européenne

1.1.1. Démarche de gestion des sédiments contaminés

Les sédiments contaminés peuvent poser de graves problèmes aussi bien pour la santé humaine que pour l'environnement, constituant une source importante de produits chimiques et présentant un danger pour les populations et les organismes aquatiques. L'exposition humaine résulte d'un contact direct, par consommation de poissons ou de coquillages ayant ingéré des produits toxiques ou l'eau exposée à des sédiments contaminés. Les organismes aquatiques, particulièrement les espèces benthiques[11], sont exposés de façon continuelle aux contaminants se trouvant dans les sédiments, qui peuvent avoir des effets néfastes incluant des toxicités aiguës et chroniques. L'accumulation de produits chimiques toxiques au sein des organismes aquatiques peut être suffisante pour les rendre impropres à toute consommation humaine et constituer une menace pour la vie sauvage. Afin de préserver l'environnement, les contaminants contenus dans les sédiments doivent être traités d'une façon à éviter ou à limiter les expositions éventuelles des populations et des organismes aquatiques. De plus, la dégradation de la qualité d'un sédiment doit aussi être prise en compte.

Les techniques d'isolement des contaminants dans les sédiments vont des solutions naturelles par enterrement à l'élimination et au traitement du sédiment en l'isolant du reste de l'environnement. Lorsque les sédiments contaminés se trouvent

11 Selon le Larousse, l'adjectif « benthique » signifie « relatif au fond des mers ou des eaux douces, quelle qu'en soit la profondeur ».

dans des zones devant être drainées pour maintenir une certaine navigabilité, la suppression du sédiment est en pratique la seule option, mais le traitement devient dans ce cas problématique.

La figure 19 présente la démarche globale de traitement des sédiments contaminés proposée par l'Agence américaine de protection de l'environnement (*Environmental Protection Agency*, EPA), démarche reprise dans la plupart des pays impliqués dans un processus de traitement des sédiments contaminés. Le processus d'identification-évaluation-traitement des sédiments contaminés est divisé en cinq phases par l'EPA :

- détection des sources de décontamination ;
- évaluation de la contamination ;
- prévention et contrôle des sources de contamination ;
- traitement des sédiments contaminés ;
- gestion du sédiment.

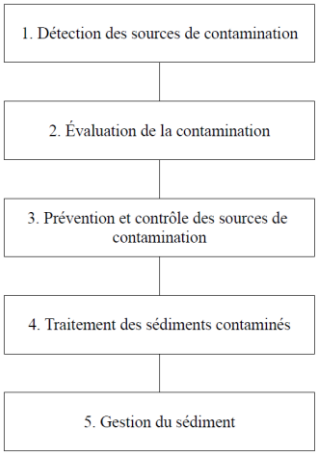


Figure 19 ■ Démarche générale de traitement des sédiments contaminés

► **ÉTAPE 1 —**

La contamination de sédiments est un processus influencé par de nombreuses variables incluant des sources de contamination, des types de contaminants, l'environnement sédimentaire et hydrologique, la taille, la composition et la répartition du grain sédimentaire ainsi que la présence ou non de vie aquatique.

La probabilité pour qu'une contamination devienne un problème sur un site particulier doit être évaluée en se fondant sur des informations récentes. De telles informations peuvent provenir d'un suivi de programmes de réhabilitation de site, d'études précédentes sur site, d'enregistrements de drainages passés, de pêches effectuées ou de zonages géographiques. Il est intéressant de noter que la contamination des sédiments est très souvent liée à une très mauvaise qualité des eaux. La capacité des sédiments à retenir les contaminants leur confère un taux de contamination supérieur aux normes de contamination des eaux.

► ÉTAPE 2 — ÉVALUATION DE LA CONTAMINATION

La deuxième étape concerne l'évaluation de la contamination. Lorsqu'une analyse préliminaire indique un possible problème de contamination, une caractérisation du sédiment plus complète est nécessaire, incluant une évaluation de la « menace » environnementale posée par la contamination. Dans le choix des méthodes d'évaluation du sédiment, la protection doit être considérée en premier lieu. Les méthodes d'évaluation peuvent varier selon les objectifs à évaluer, qu'il s'agisse des effets sur la vie aquatique et sauvage ou des effets sur la santé humaine.

L'évaluation la plus simple compare directement les concentrations de contaminants de sédiments observées avec quelques critères préétablis. Les critères de qualité des sédiments sont plus difficiles à mettre en place que des critères portant sur la qualité des eaux en raison du nombre et de la grande complexité des facteurs pouvant affecter les effets biologiques engendrés par la concentration d'un produit chimique donné.

Les effets des sédiments, définis en considérant les connaissances scientifiques actuelles, embrassent :

- le type et l'étendue de tous les effets identifiables sur la santé et le bien-être, et non les effets limités au plancton, aux poissons, aux crustacés, à la vie sauvage pouvant être touchés par la contamination des sédiments ;
- la concentration et la répartition des polluants à travers des processus biologiques, physiques et chimiques ;
- les effets des polluants sur la diversité biologique.

► ÉTAPE 3 — PRÉVENTION ET CONTRÔLE DES SOURCES DE CONTAMINATION

La troisième étape concerne la prévention et le contrôle des sources de contamination. Il est important de déterminer l'origine de toute contamination nouvellement découverte. Le type d'actions à entreprendre dépend partiellement de l'ampleur de la contamination : si un contaminant est identifié sur de nombreux sites géographiques, il sera vraisemblablement inefficace de ne gérer qu'un seul site. La gestion des sédiments contaminés requiert une approche globale. Les sources de contamination sont probablement si nombreuses qu'une action isolée (par exemple, sur une seule décharge) a toutes les chances de demeurer inefficace. Il est alors plus pertinent de passer par un programme global et systémique de traitement et par l'établissement de réglementations spécifiques. Par ailleurs, la contamination d'un seul site peut nécessiter un contrôle local et des contrôles de grande ampleur peuvent s'avérer inappropriés ou moins efficaces.

La détermination du lieu de la contamination ainsi que son ampleur marque le début de cette étape.

Malgré tout, même en présence de démarches nationales, régionales ou locales pour le traitement de contaminants, chaque site reste unique dans sa configuration et dans sa composition. Il est donc nécessaire de faire du « cas par cas » dans la plupart

des situations. Certains points sensibles demandent une démarche spécifique pour lesquels une prise de mesures de contrôles des sources est envisagée jusqu'à ce qu'une législation soit mise en place car tout retard pourrait engendrer des impacts environnementaux inacceptables. Il est également intéressant de noter que la présence d'un contaminant présent sur plusieurs sites géographiques n'indique pas forcément qu'une action de contrôle de grande ampleur soit entreprise. Les sédiments emmagasinent des contaminants pouvant perduraient dans celui-ci même si le déversement du contaminant a été arrêté. En fait, dans ces cas de contamination une démarche de restauration de site est privilégiée à une démarche de contrôle de la source.

Le meilleur moyen de lier une contamination de sédiment à des sources possibles est d'adopter une démarche contaminant par contaminant. Les tests de toxicité ne permettent pas d'identifier directement les problèmes des contaminants, ils peuvent jouer un rôle déterminant dans une analyse initiale pour des sédiments potentiellement contaminés et par le biais de techniques d'identification de la toxicité il sera possible d'identifier les contaminants responsables d'une toxicité observée. Les relations géographiques entre un pic de concentration d'un contaminant dans un sédiment et les possibles sources peuvent aussi être utilisées pour relier la contamination des sédiments et les sources.

Lorsque de nombreuses sources de contamination existent pour un contaminant donné des preuves supplémentaires doivent être recherchées afin de lier un contaminant à sa source. Les niveaux de concentration des contaminants peuvent être observés sur la surface sédimentaire avec une contamination maximale directement à l'endroit du déversement. De plus, le niveau de contamination peut varier selon la profondeur de relevé dans le sédiment permettant ainsi de retracer l'histoire de la contamination du sédiment. Il est donc possible de mettre en place une empreinte d'un site grâce aux occurrences ou aux concentrations pour un ou plusieurs contaminants.

Si la contamination est limitée à un seul site, le premier élément à prendre en compte est l'ancienneté de la contamination : si la source de contamination est ancienne alors le contrôle de la source peut être éliminé. Trois types de sources de contamination peuvent être distingués :

- les sources localisées, par exemple des écoulements industriels ou communaux ;
- des sources non localisées : épandages agricoles, eaux diluviennes, contaminants atmosphériques… ;
- les autres sources : déversements, réseaux d'évacuation…

► ÉTAPE 4 — TRAITEMENT DES SÉDIMENTS CONTAMINÉS

C'est sur cette étape de traitement des sédiments contaminés que le procédé Novosol® intervient (figure 20). Les sédiments ne sont pas systématiquement traités, en raison notamment :

- du manque de réglementation claire ;
- du coût élevé de traitement des sédiments contaminés ;
- du manque de critères établis afin de déterminer les niveaux d'action et de traitement.

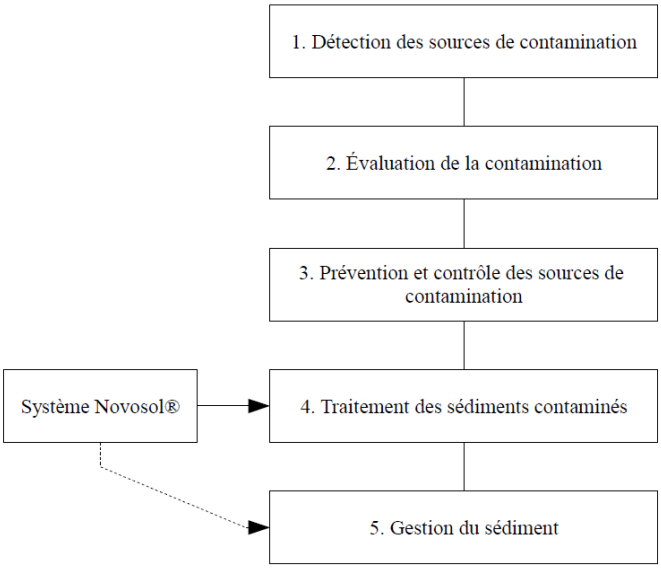


Figure 20 ■ Place du procédé Novosol® dans la démarche globale de gestion des sédiments contaminés

Les bénéfices environnementaux d'un traitement de sédiments contaminés doivent être pesés au regard des coûts du traitement et de ses impacts possibles sur l'environnement. Par exemple, il est tout à fait plausible qu'un habitat benthique soit détruit en raison d'un drainage de sédiments ou bien qu'une partie des contaminants de sédiments soit dispersée lors de ces opérations de drainage. C'est pourquoi il reste important de peser les avantages et inconvénients d'une opération de traitement tout en prenant en compte les impacts potentiels sur l'environnement.

Fondamentalement, les traitements de sédiments doivent s'efforcer d'atteindre une qualité environnementale acceptable, ne modifiant pas les processus naturels sur une période de temps raisonnable. Théoriquement, un sédiment ne correspondant pas aux critères de qualité ou ayant des impacts environnementaux néfastes doit être considéré comme inacceptable. Dans tous les cas, l'information nécessaire pour décider ou non d'un traitement doit répondre aux principales questions suivantes [US-EPA, 2005] :

- le sédiment contaminé pourra-t-il être traité dans un délai acceptable ?
- les sédiments traités seront-ils dispersés naturellement ou par un autre mécanisme ?
- le sédiment contaminé pose-t-il un danger pour des zones éloignées ?
- des alternatives techniquement et économiquement faisables existent-elles pour le traitement des sédiments contaminés ?

- les effets positifs à long terme du traitement sur l'environnement sont-ils bénéfiques par rapport aux effets néfastes à court terme ?

En réponse à ces questions, il existe en général trois options de traitement des sédiments contaminés (figure 21) :

- ne prendre aucune mesure et laisser perdurer la sédimentation naturelle ;
- traiter les sédiments contaminés sur place ;
- enfin, draguer les sédiments contaminés et les envoyer sur un autre site pour traitement ou non.

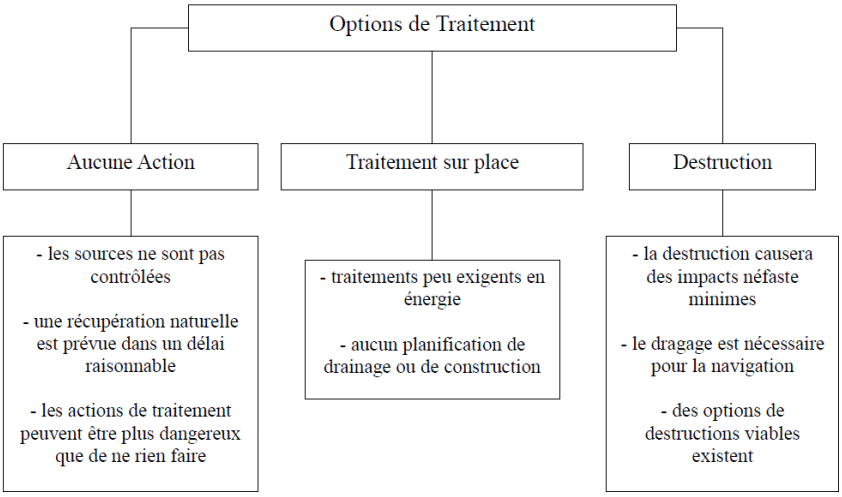


Figure 21 ■ Options de Traitement
Source : US-EPA

Il peut être opportun de combiner différentes options. Ainsi, il est possible de draguer les sédiments dans une partie d'un site mais de les traiter dans une autre partie du site. En règle générale, les bénéfices environnementaux attendus, les impacts néfastes possibles sur la santé et l'environnement, le temps naturel de décontamination ainsi que la faisabilité et le coût des différents traitements sont les principaux critères de décision des options.

Concernant les différentes options de traitement, si la destruction consiste en premier lieu à réduire les risques sanitaires et environnementaux, les sédiments laissés sur place sont probablement plus contaminés que ceux drainés. Ainsi, différents degrés de traitement peuvent être requis avant la destruction du sédiment. Dans certains cas, il est possible de séparer les sédiments et les résidus de traitement en fractions « contaminée » et « non contaminée ». Ainsi, seule la fraction contaminée devra être stockée dans une zone protégée alors que les sédiments traités pourront être valorisés. Cette séparation des sédiments contaminés et non contaminés est commune à plusieurs technologies de traitement des sédiments contaminés, par exemple les technologies détruisant les contaminants par calcination (cf. procédé Novosol®). Cependant, pour abaisser les coûts, les technologies de traitement des sédiments contaminés doivent se montrer capables d'abaisser les concentrations

chimiques des contaminants dans les sédiments traités jusqu'à des niveaux acceptables.

Sans entrer dans les détails, les options de traitement de sédiments contaminés se répartissent en cinq catégories :

- réduction du volume de sédiments contaminés ;
- neutralisation du contaminant ;
- destruction du contaminant ;
- extraction du contaminant ;
- séparation thermique.

► ÉTAPE 5 — GESTION DU SÉDIMENT

La phase de traitement doit donc être immédiatement suivie d'une phase de gestion des sédiments, qui comporte quatre modalités :

- le déversement aquatique des sédiments décontaminés ou non contaminés ;
- la valorisation des sédiments, pouvant se traduire par des constructions de digues ou dans le cas du processus Novosol®, de remblais de route par utilisation de sédiments traités ou décontaminés ;
- un déversement aquatique afin de confiner les sédiments contaminés par recouvrement sur un site aquatique ou en stockage sur site étanche ;
- la construction d'une installation dédiée aux sédiments hautement contaminés, dont le traitement est susceptible d'émettre des rejets atmosphériques.

Ce processus de gestion des sédiments contaminés intègre différentes techniques de traitement présentées ci-après.

1.1.2. Différentes techniques de traitement des sédiments contaminés

Le traitement des sédiments contaminés impose des défis technologiques, économiques et environnementaux de plus en plus importants. Il permet d'atteindre des teneurs en polluants acceptables pour que les sédiments contaminés puissent éventuellement être réutilisés. Une phase de caractérisation du sédiment permet de choisir la technologie adéquate et surtout d'en estimer le coût. En effet, certaines techniques de traitement peuvent avoir des impacts environnementaux dus à des rejets d'eau et/ou de gaz.

Le tableau 8 regroupe la plupart des techniques conventionnelles de traitement des sédiments contaminés applicables. Il est à souligner qu'aucune technique de traitement de sédiments contaminés ne peut éliminer, stocker ou traiter un sédiment contaminé sans perturbations et sans relâchement de contaminants lors des manœuvres. Les perturbations appliquées au système sédimentaire se trouvant au fond d'un site aquatique peuvent causer une mise en suspension de contaminants

dans la colonne d'eau, dont la solution de traitement devra s'assurer qu'elle est la plus faible possible.

Techniques de traitement	Application	Caractéristiques	Efficacité	Coût
Traitement biologique				
	pesticides, hydrocarbures, PCB, aromatiques chlorés	pH de 4,5 à 8,5 température de 59 à 167 °C hydratation de 40 à 80 %	dépend du volume de traitement	moyennement élevé
Traitement physico-chimique				
Déchloration	dioxines, PCB, Chlorobenzène	pH > 2 température de 158 à 302 °C hydratation < 20 %	efficacité > 98 % pour les PCB	élevé
Extraction par solvant	PCB, composés organiques volatils, aromatiques, métaux	composés organiques < 40 % portion solide < 20%	efficacité d'environ 90 % pur les PCB	élevé
Lessivage des sols	métaux lourds, aromatiques, PCB, pesticides	taille des particules 0,063-2 mm	90-99 % des volatils et entre 40 et 90 % pour les semi-volatils	élevé
Solidification/stabilisation	composés inorganiques, boues huileuse et solvants		totalement efficace sur composés inorganiques	peu élevé
Traitement thermique				
Calcination	composés volatils et semi-volatils, dioxines	hydratation < 50 % taille de particules 1-2 mm	plus de 99 % pour les composés organiques	très élevé
Désorption à basse température	composés volatils et semi-volatils		99 %	élevé

Tableau 8 ■ Techniques de traitement de sédiments contaminés
Source : US-EPA

La sélection des traitements privilégie ceux qu'il est possible d'appliquer *in situ*, car la limitation des transports et des risques induite permet une sensible baisse des coûts. Néanmoins, un traitement sur site demande un espace conséquent, condition rarement remplie.

Dans la majorité des cas, le sédiment est dragué, puis stocké ou traité *ex situ*. Le principal avantage d'un traitement *ex situ* est sa forte acceptation sociale malgré des coûts plus importants dus à l'extraction, au transport et au traitement. Le retrait et le transport des sédiments contaminés constituent toutefois des étapes délicates, risquant d'introduire des contaminants sur un site jusque là indemne. La décision de dragage dépend de la nature du sédiment, de la profondeur du site aquatique, de l'épaisseur et du volume du sédiment, de la distance du site de traitement et du matériel opérationnel à disposition ; quant aux techniques de dragage, il en existe trois principales : mécanique, hydraulique et pneumatique. La méthode de transport de produits dragués dépend de la distance entre les sites de dragage et de traitement. Les principales techniques de transport recourent aux « pipelines », aux barges, au chemin de fer et aux camions. La sélection du mode de transport jusqu'au site de traitement dépend de la technique de dragage et du choix de traitement des sédiments contaminés.

Après cette phase de dragage et de transport, le sédiment dragué subit une phase de prétraitement passant notamment par une élimination du surplus en eau et par un tri des particules afin d'éliminer les granulométries trop importantes. Une phase de prétraitement du sédiment contaminé présente quatre avantages en raison de la capacité des contaminants à se fixer sur les fines[12] :

- réduire la teneur en eau afin de faciliter le transport vers un lieu de stockage ou de traitement ;
- réduire le volume de sédiments à traiter ou à placer en sites confinés ;
- permettre de favoriser ou d'accélérer la sédimentation des parties solides et de séparer les matériaux valorisables de ceux devant être traités ou mis en dépôt ;
- enfin, permettre de trier les matériaux en différentes catégories répondant à différents types de traitement.

L'élimination de l'eau contenue dans le sédiment rapproche sa manipulation et son transport de ceux d'une matière solide, et prépare le sédiment aux étapes de traitement. Cette phase de suppression du surplus d'eau est généralement efficace et peu coûteuse mais requiert du temps et un espace conséquent. Les méthodes usuelles sont la centrifugation, la filtration ou la suppression par gravité. Des produits chimiques comme des floculents peuvent être ajoutés pour accélérer le dépôt des particules solides en suspension. L'étape de tamisage des particules permet de séparer les particules sédimentaires selon leurs propriétés physiques (taille, densité,

12 Selon le Larousse, « morceaux de minerais de dimension millimétrique, souvent séparés par criblage pour être traités à part ou agglomérés ».

masse…), la partie grossière pouvant être réutilisée, après avoir été analysée, comme remblais ou bien comme matériau de construction. Cette démarche peut engendrer d'importantes économies de dépollution.

L'objectif fondamental du procédé Novosol®, comme de tout traitement de sédiments contaminés, est d'extraire, immobiliser, détruire ou neutraliser les contaminants. Les différentes techniques de traitement présentent chacune des avantages mais aussi des inconvénients, principalement dus à une limitation dans le nombre de contaminants traités (certaines techniques ne traitant qu'une catégorie de contaminants). De plus, l'intégration d'une technique particulière dans le processus de traitement engendre des difficultés et des coûts supplémentaires. Ainsi, divers critères influent sur le choix d'une méthode de traitement : propension des contaminants à la lixiviation[13], stabilité des contaminants, caractérisation des sédiments et de leurs contaminants, homogénéité des sédiments et impacts environnementaux sociaux et sanitaires. Parmi les trois grandes classes de traitements (biologique, physico-chimique, ou de stabilisation — *v.* tableau 8), certains sont utilisés dans le cadre de l'application du procédé Novosol®, décrit ci-dessous.

2. Le système Novosol®

Les étapes du procédé Novosol®, développé par le groupe Solvay SA, combinent différentes techniques de traitement de sédiments contaminés afin de stabiliser les résidus minéraux contaminés par des métaux lourds et des composés organiques. Ce procédé constitue un système tel que défini par Bertalanffy [Bertalanffy, 1968].

Novosol® intègre des technologies innovantes pour répondre aux différentes problématiques du procédé. Ainsi, il exploite le procédé Neutrec®[14] développé également par le groupe Solvay SA pour l'épuration des fumées émises lors de l'exploitation Novosol® [Novosol®, 2010].

Cette section est organisée en deux sous-sections. Une première vise à décrire le procédé technique Novosol® centré sur le processus physico-chimique de traitement, la seconde présente le système socio-technique Novosol®, composé des différents

13 Selon Le Larousse, « opération qui consiste à faire passer lentement un solvant à travers un produit convenablement pulvérisé et déposé en couche épaisse, pour en extraire un ou plusieurs constituants solubles » ou « Dissolution chimique de certains constituants d'un matériau utilisée pour extraire d'un minerai, les métaux, les minéraux de valeur ».

14 Le procédé Neutrec® est « basé sur l'injection à sec de bicarbonate de sodium finement broyé dans les fumées à épurer. Le bicarbonate de sodium neutralise les acides (acide chlorhydrique, dioxyde de soufre, acide fluorhydrique…) avec une très grande efficacité. Moyennant l'injection combinée de charbon actif ou de coke de lignite, les fumées sont également épurées en métaux lourds et en dioxines / furannes, en respectant les législations les plus sévères. Le procédé étant totalement sec, aucun effluent aqueux n'est généré et ne doit être traité. »

acteurs intégrant aussi bien la phase de développement du procédé que la phase d'exploitation.

2.1. Le procédé Novosol®

Le procédé Novosol® constitue l'aboutissement de quinze années de recherche dans le domaine de la stabilisation des résidus minéraux contaminés par des métaux lourds et des composés organiques.

À partir de 1993, le groupe Solvay SA a débuté le développement du procédé Novosol® [Depelsenaire, 2006] afin de traiter efficacement tout d'abord les cendres volantes d'incinération puis, à partir de 1999, une large gamme de sédiments contaminés. Ce développement a débuté en partenariat avec l'Université libre de Bruxelles [Breugelmans, 2007]. Ce procédé répondait à un besoin de la Région wallonne belge de traiter des sédiments contaminés par des métaux lourds.

Ce procédé est divisé en deux étapes de traitement [Novosol®, 2010] : une étape de phosphatation suivie d'une étape de calcination. Après des premiers résultats prometteurs et le dépôt de brevets[15], les recherches se sont poursuivies au sein du centre de recherche de Solvay. Parallèlement à ces recherches, d'autres travaux ont été menés en collaboration avec des partenaires institutionnels et académiques, faisant l'objet de thèses de doctorat.

En 2004, les résultats concluants ont mené à la construction d'un pilote industriel grâce à une collaboration avec des partenaires institutionnels et industriels.

Un an plus tard, une seconde partie du pilote industriel était exploitée dans une des installations du groupe Solvay. À la fin de l'année 2005, une « route test » d'une longueur de 100 mètres a été construite dans le cadre une revalorisation des sédiments traités en partenariat avec une société de construction routière et incorporant 30 % de sédiments fluviaux. Par ailleurs, des sédiments traités par le procédé Novosol® ont été incorporés à hauteur de 25 % pour la production de briques.

L'ingénierie de base d'une installation complète a été terminée à la fin 2006 et une installation industrielle construite par les partenaires de Solvay SA est prévue en 2011.

En 2010, le système Novosol® a été concédé sous forme de licences d'exploitation limitées dans le temps et l'espace à deux entreprises d'exploitation, SEDISOL[16] et SIFA. Chacune de ces entreprises est une « entreprise exploitante Novosol® », qui va exploiter la technologie Novosol® à des fins de traitement de sédiments contaminés.

15 Brevets :
– en Europe : EP 0883585 B1 (12 janvier 2000) et EP 0899000 B1 (3 novembre 2004) ;
– aux États-Unis : 6 132 355 (17 octobre 2000) et 6 254 846 (3 juillet 2001).

16 http://www.sedisol.be/inauguration/index.php

Pour chacune des entreprises exploitantes, des entreprises en charge du développement d'un site Novosol® font l'objet d'un partenariat industriel. Respectivement, SEDISOL collabore avec SERIP[17] et SIFA coopère avec Studio Altieri[18]. En effet, Solvay ne cède que des licences et n'exploitera ou ne construira aucune installation Novosol®.

Le procédé Novosol® apporte une réponse au traitement des résidus minéraux, chargés en métaux lourds et en matières organiques. Ces résidus recouvrent non seulement des sédiments pollués des canaux et des ports, mais également des résidus d'activités gérées par les pouvoirs publics et les collectivités locales comme les cendres volantes des incinérateurs d'ordures ménagères. Ces résidus peuvent également provenir d'activités relevant d'entreprises privées et concerner les résidus de broyage des automobiles ou bien des boues industrielles. Ces domaines peuvent générer de nombreux résidus pollués dont le traitement peut, au-delà d'une simple protection environnementale, s'avérer une nécessité absolue.

Le procédé Novosol® comporte deux phases de traitement : une phase de phosphatation, puis une phase de calcination.

2.1.1. La phase de phosphatation

La première étape du procédé Novosol® est une phase de phosphatation (figures 22 et 23), chargée d'assurer la stabilisation et la réduction de la solubilité des métaux lourds dans les sédiments contaminés par ajout d'acide phosphorique.

D'un point de vue opérationnel, le dimensionnement de l'unité permet de traiter 100 000 m^3/an de sédiments bruts à 50 % d'humidité pendant 200 jours par an et 5 jours par semaine. Pour cela, le fonctionnement à 100 m^3/h est effectif pendant 5 h par jour et ne nécessite que la présence d'opérateurs de jour.

Cette phase de phosphatation se divise en plusieurs étapes lorsqu'elle se trouve en fonctionnement. Chacune de ces étapes est sous la responsabilité des opérateurs au nombre de trois (désignés par les trois lettres A, B et C) et d'un chef d'équipe conformément à l'ingénierie définie par Solvay (figures 22 et 23).

Chacun des opérateurs possède au sein du site Novosol® une ou plusieurs zones de compétence auxquelles se rattachent des tâches opérationnelles.

L'opérateur A (zones vertes sur figures 22 et 23) est en charge :

- du dégrillage ;
- du stockage ;
- du pompage et de la phosphatation des sédiments ;
- de la mesure de la masse volumique des sédiments ;

17 http://serip-france.pagesperso-orange.fr/accueil_070.htm

18 http://www.studioaltieri.it/

- du traitement des gaz.

L'opérateur B (zone bleue sur les figures 22 et 23) est en charge :

- de la gestion des sédiments phosphatés ;
- des bassins de stockage des liquides.

L'opérateur C (zone jaune sur les figures 22 et 23) est en charge :

- des utilités ;
- du chargement des camions ;
- de la logistique d'approvisionnement et d'expédition.

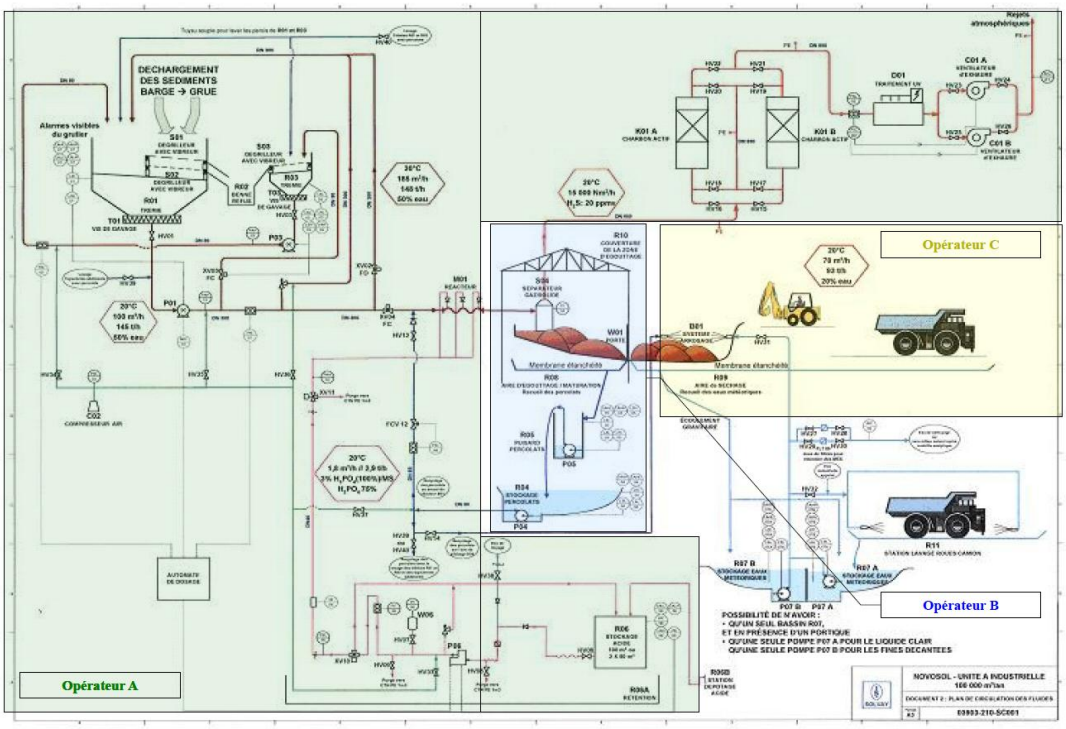


Figure 22 ■ Diagramme de flux Novosol® lors de la phase de phosphatation organisé en fonction des zones de responsabilité de chaque opérateur
source : Solvay SA

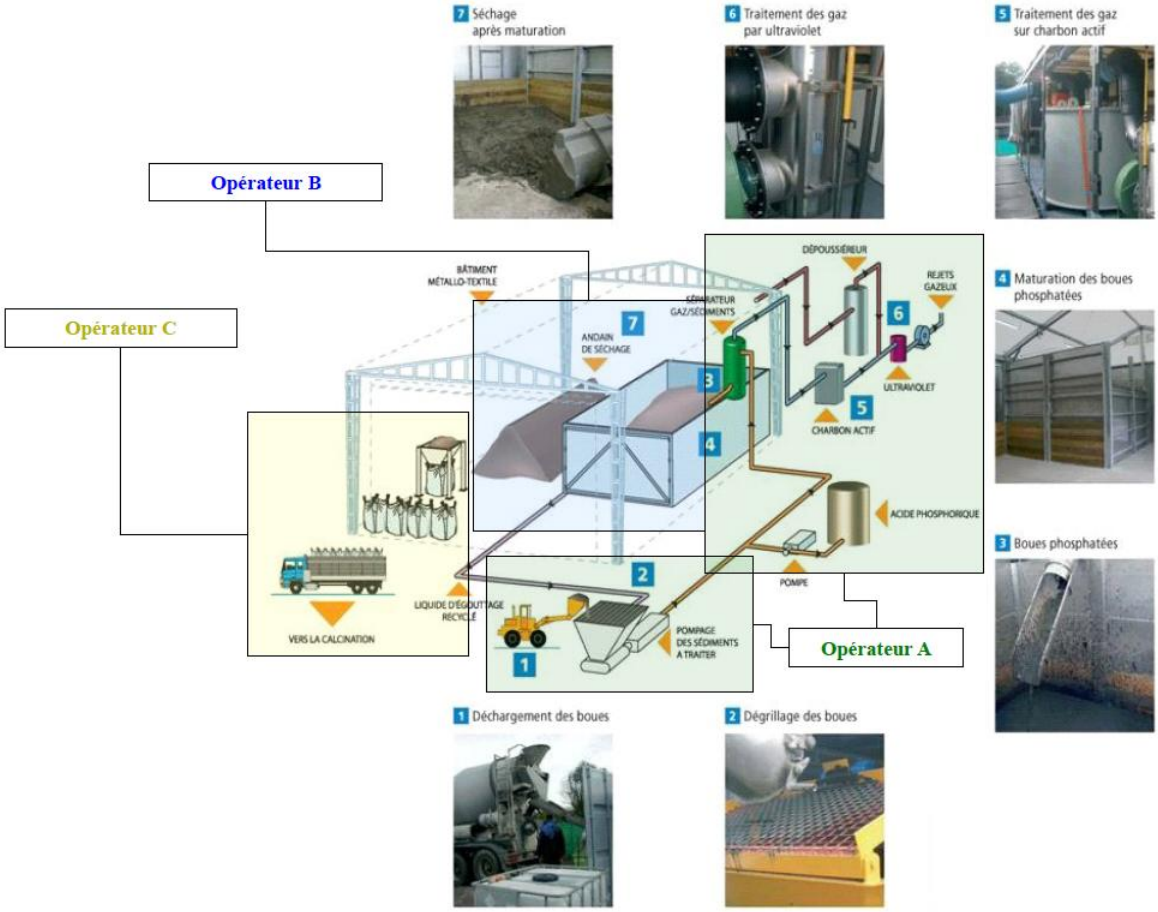


Figure 23 ■ Étape de phosphatation du procédé Novosol® illustrée en fonction des zones de responsabilité de chaque opérateur
source : Solvay SA et conforme à la figure 22

Au delà de ces considérations, le procédé est actuellement principalement utilisé pour le traitement des boues de dragage et s'insère dans une démarche globale de gestion des sédiments contaminés (*v.* figure 20). En effet, l'envasement des cours d'eau et des zones portuaires est un véritable obstacle à la navigation fluviale. Cet envasement peut accentuer les risques d'inondation en cas de crue ou même de pollution de l'eau potable des collectivités. La solution la plus courante est alors le dragage, c'est-à-dire l'extraction des sédiments aux endroits où ils se sont accumulés. Ces sédiments sont très souvent chargés en polluants issus des rejets urbains, industriels et agricoles.

Le traitement des métaux lourds des sédiments se fait par adjonction d'acide phosphorique, formant ainsi du phosphate de calcium. Après phosphatation les matériaux sont stockés durant 24 h sur un géotextile drainant puis déversés en andains de séchage. Cette phase de maturation permet une réduction de la teneur en eau de 40 % avec une immobilisation des métaux lourds. Un système d'épuration des gaz est également inclus grâce à une filtration par charbons actifs et à un lavage.

Cette phase de phosphatation peut être suivie, de façon facultative et selon les besoins industriels, d'une phase de calcination.

2.1.2. La phase de calcination

La matière organique issue de l'étape de phosphatation peut être détruite par calcination (figure 24).

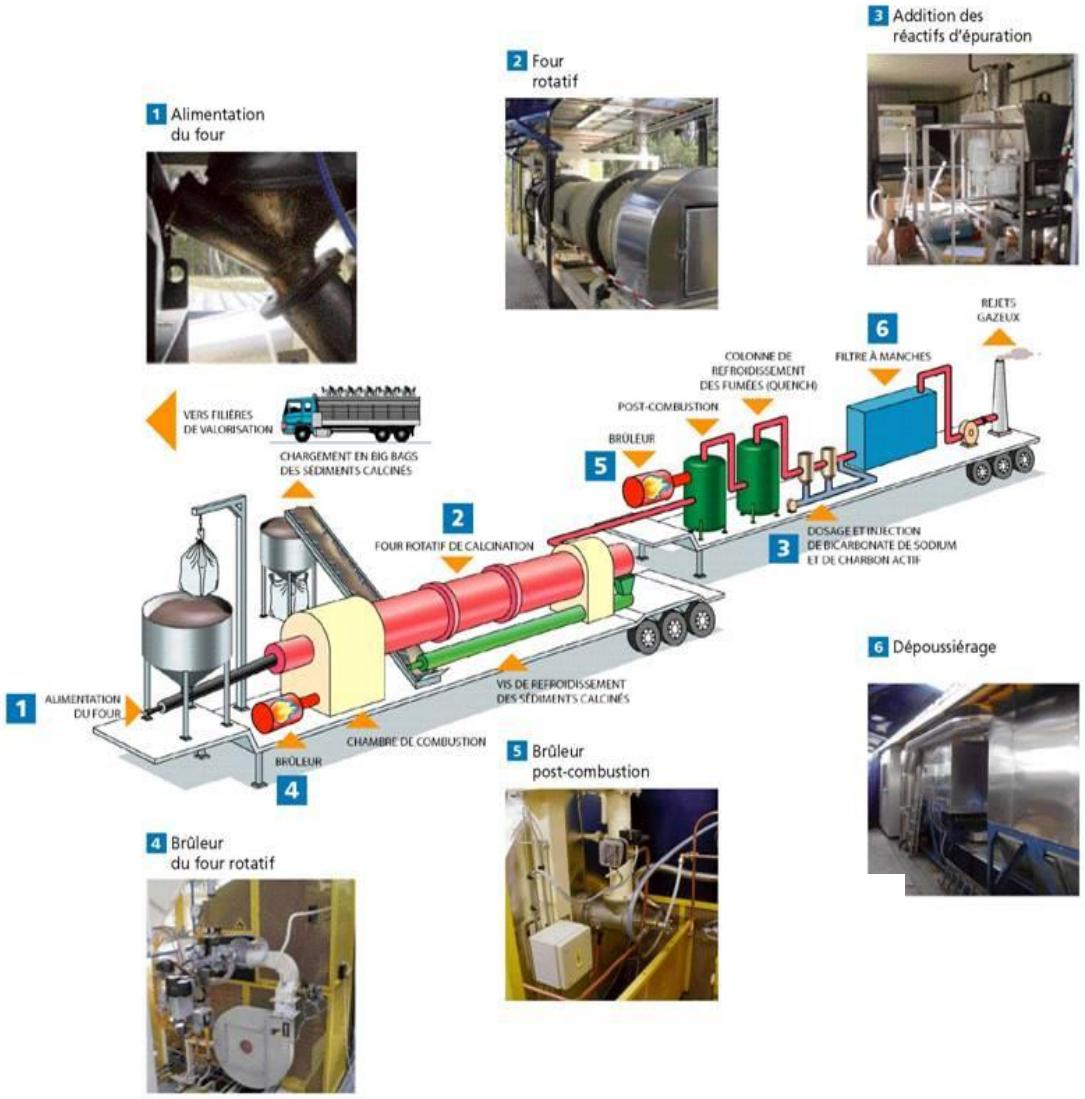


Figure 24 ■ Étape de calcination du procédé Novosol®
source : Solvay SA

L'étape de calcination permet de renforcer la stabilisation des métaux lourds résultant de la phosphatation et surtout de fournir des produits susceptibles d'être valorisés. La calcination permet également la destruction des composés organiques. C'est au cours de la phase de calcination que le procédé Neutrec® est intégré afin d'épurer les fumées issues de la calcination des sédiments.

Plusieurs unités pilotes du procédé Novosol® ont été construites afin de procéder à divers tests de confirmation des performances du procédé et d'évaluation des coûts d'investissement et de fonctionnement. Ces unités permettent aussi de conforter la valorisation des résidus traités (construction de digues et de routes, fabrication de briques…), qui évite la mise en décharge. Ces voies de valorisation ont été complétées récemment par le développement de ciment à base de résidus traités grâce à la technologie Novosol®.

Le procédé Novosol® est mis à la disposition des pouvoirs publics et des acteurs industriels sous la forme d'une licence d'exploitation, tout en conservant un lien fort avec les différents partenaires, qui favorise la poursuite du développement du procédé avec le soutien d'équipes d'experts. Ce réseau d'acteurs est à l'origine du projet SEDIMARD (« Sédiments marins dragués contaminés »), initié par le conseil général du Var pour un montant d'environ 1,7 million d'euros et ayant mené à l'élaboration par SEDISOL d'un pilote en Belgique.

2.2. La description du système Novosol®

L'analyse effectuée ici est centrée sur l'étape de phosphatation, conformément aux exigences industrielles formulées par le groupe Solvay SA. La phase de calcination est donc sciemment écartée.

D'un point de vue strictement technique, la dynamique du procédé Novosol® reste simple (figure 25).

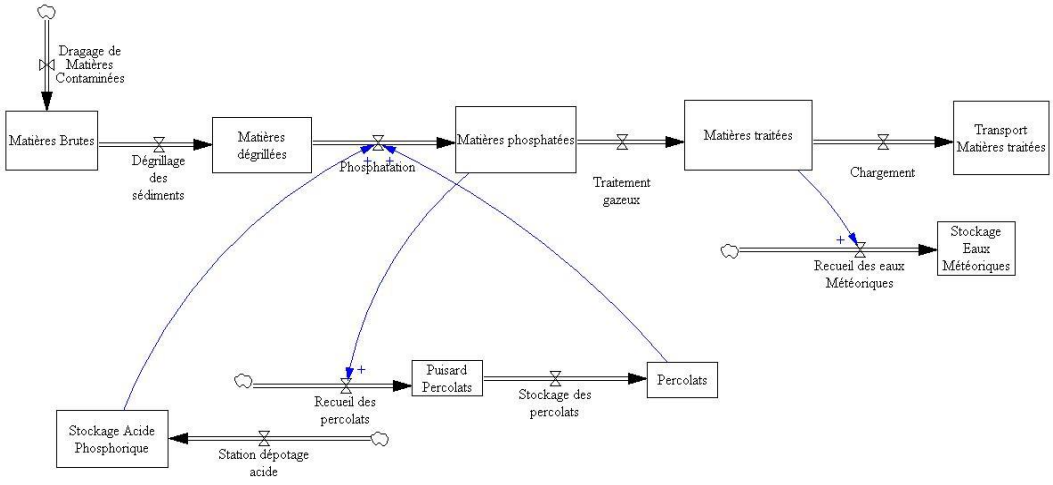


Figure 25 ■ Modèle dynamique de la phase de phosphatation du système technique Novosol®

Par ailleurs, le procédé est quantifiable afin de permettre l'application de scénarios d'étude de son fonctionnement et de son comportement. Néanmoins, l'objet du présent travail de thèse ne se restreint pas au sous-système technique : il s'agit bel et bien d'adopter une vision d'ensemble de ce procédé, au sein d'un système global

dans lequel l'ensemble des interactions sont prises en compte — notamment les facteurs humain et organisationnel.

Cette hauteur d'analyse se retrouve dans le modèle représentant la dynamique du système Novosol® centrée sur la sécurité, dans un souci de performance conformément aux démarches en sécurité des systèmes (figure 26). Ce modèle dynamique inclut l'ensemble des variables définies lors de l'application du modèle STAMP permettant de mieux cerner l'ensemble des interactions du système global (tableau 9).

L'ensemble ainsi défini s'inscrit dans une démarche d'amélioration de la performance par une gestion des risques et de la sécurité au sein du système. Ce modèle dynamique peut être à l'origine de discussions portant sur l'optimisation de la sécurité ou sur l'évaluation de la sécurité, traitées dans le prochain chapitre.

Variables structurelles du système Novosol®	
Liées à un niveau de performances (niveau hiérarchique)	**Liées à un niveau de qualité (contrôles)**
Direction de l'exploitation	Réglementation
Direction du développement	Exigences de développement
Management du développement	Rapports de développement
Développeurs	Documentation et ingénierie
Conception et acquisition	Évaluation des dangers en conception
Maintenance et évolution	Rapports d'exploitation et d'incidents
Management de l'exploitation	Procédures d'exploitation
	Évaluation des dangers en exploitation
	Formations des opérateurs
	Procédures de développement
	Formation des développeurs

Tableau 9 ■ Variables structurelle du système Novosol®

La description donnée du système Novosol® (figure 27) est un modèle statique focalisé sur la structure du système global Novosol® mettant en exergue ses hiérarchies ainsi que ses différentes interactions. Ce schéma a été construit conformément à l'étape 2 de la méthode STPA au sein de la phase statique (*v.* chapitre 3) en considérant l'ensemble des acteurs sociaux impliqués dans le système Novosol®.

Ce modèle statique, essentiel dans la détermination des hiérarchies et des interactions entre les éléments, sert de point de départ pour l'établissement d'un modèle dynamique. En effet, le modèle statique regroupe l'ensemble des variables retenues lors de la définition de la problématique et autorise ainsi l'élaboration d'un

modèle selon l'objectif fixé — ici, une évaluation de la sécurité dans un souci d'optimisation et de performance du système Novosol®.

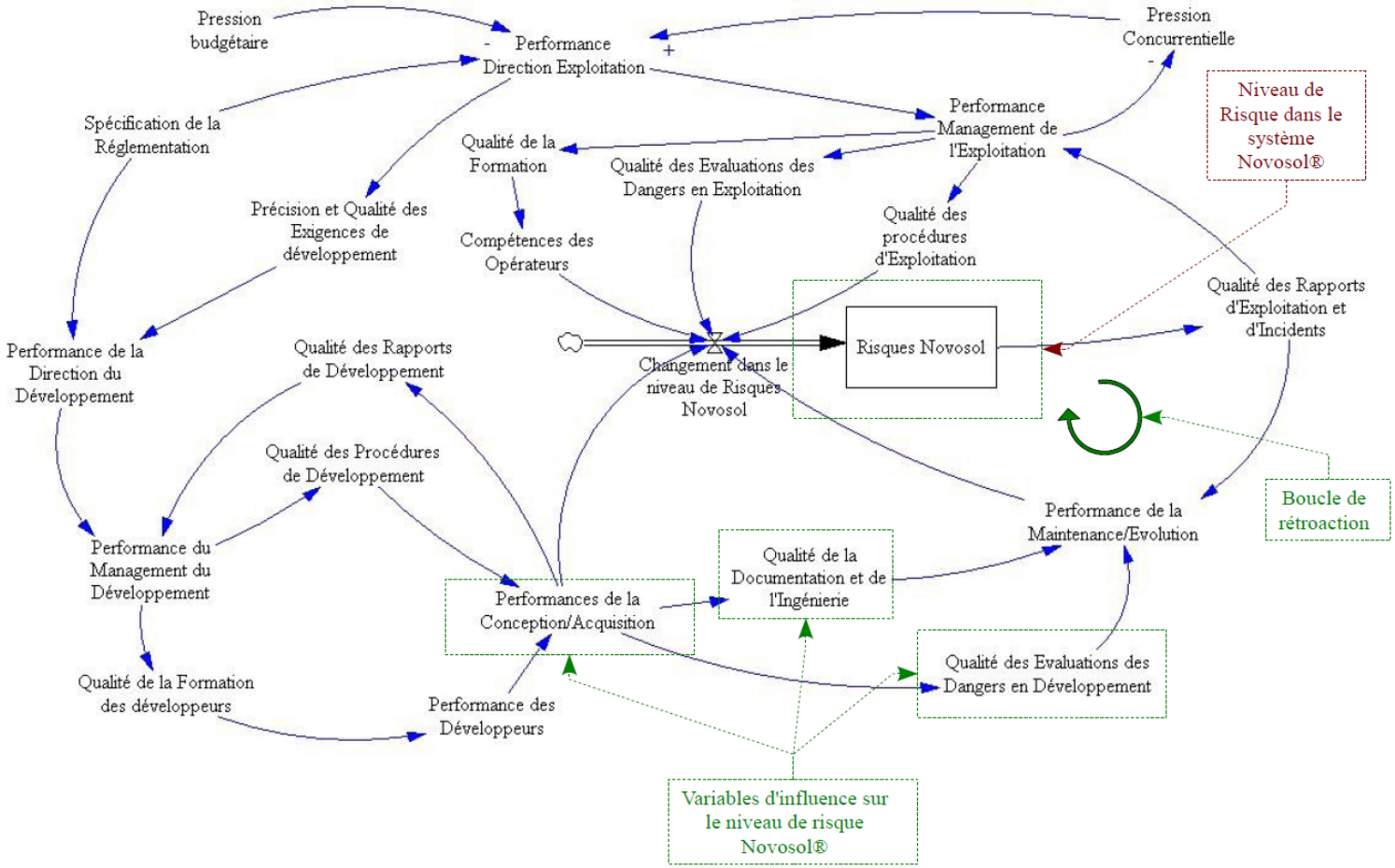


Figure 26 ■ Influences au sein du système Novosol en phase de développement et d'exploitation, centré sur le niveau de risque

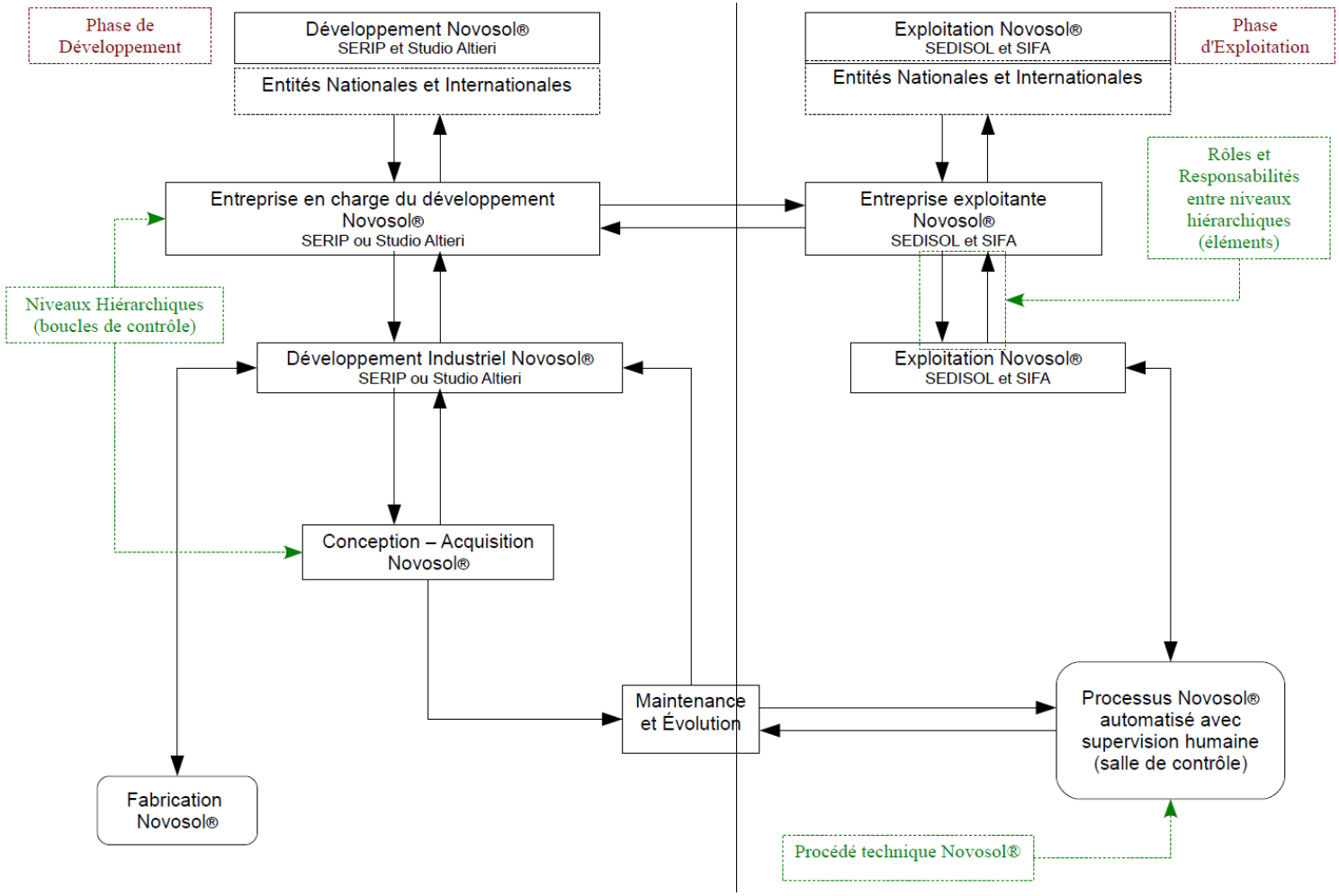


Figure 27 ■ Description générale de la structure du système Novosol®.

Cette structure décrit les niveaux hiérarchiques du système Novosol® et met en évidence l'ensemble des interactions entre les acteurs du système. Cette hiérarchisation du système sert de support pour la définition des rôles et des responsabilités (contrôles) qui interviennent entre niveaux.

3. Application de la technique d'analyse des dangers STPA

Préalablement à ce travail d'analyse, Solvay SA a défini des exigences de sécurité, ainsi formulées :

- appliquer une démarche en gestion des risques visant à éliminer les risques du procédé Novosol® pour atteindre un niveau de risque acceptable ;
- formuler des recommandations visant à améliorer le niveau de risques pour optimiser la sécurité en prenant en considération des exigences de performance, de coût et de temps.

La démarche adoptée a consisté à mettre en place des exigences globales de sécurité intégrées grâce à l'application de la technique d'analyse STPA dans le système Novosol®. Cette démarche a pour objectif l'amélioration du niveau de sécurité du système Novosol® tout au long de son cycle de vie[19]. Le système Novosol® présente des contrôles potentiellement inadéquats (évaluation des dangers non effectuée, opérateurs non formés, procédures d'exploitation non ou mal définies…) à plusieurs niveaux hiérarchiques, pouvant avoir un impact sur le niveau de sécurité global du système.

Afin de répondre à ce besoin de sécurité, la technique d'analyse STPA est appliquée ici conformément à la méthodologie présentée dans le chapitre 3. Sont donc ici appliquées les différentes étapes de la technique d'analyse des dangers STPA (figure 28) au sein du système Novosol®.

19 L'ensemble des rapports et des résultants d'analyse des risques pour le procédé Novosol® destinés à l'usage industriel de Solvay ont été fournis en 2009 sous la forme d'un rapport « papier » pour l'analyse HAZOP et d'un dvd contenant l'analyse HAZOP avec les recommandations ainsi que l'évaluation des risques professionnels.

Ces versions délivrées sont modifiables et permettent une mise à jour tout au long du cycle de vie du système Novosol®.

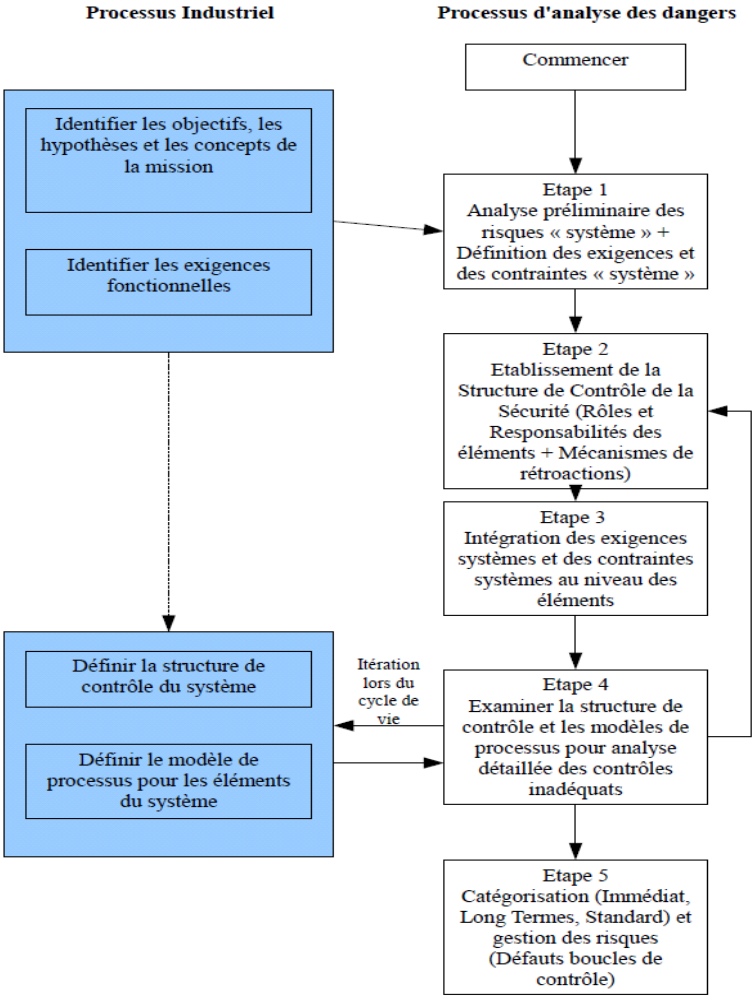


Figure 28 ■ Processus STPA en évaluation de la sécurité
adapté de Leveson et Daouk [Leveson, Daouk, 2004]

La technique d'analyse STPA comporte cinq étapes :

- étape 1 : analyse préliminaire des risques « système » et définition des exigences et des contraintes « système » ;
- étape 2 : établissement de la structure de contrôle de la sécurité (rôles et responsabilités des éléments et mécanismes de rétroaction) ;
- étape 3 : intégration des exigences « système » et des contraintes « système » au niveau des éléments ;
- étape 4 : examen de la structure de contrôle et des modèles de processus pour analyse détaillée des contrôles inadéquats ;
- étape 5 : catégorisation (immédiat, long terme, standard) et gestion des risques (défauts de boucles de contrôle),

ici reprises et appliquées au système Novosol®.

► ÉTAPE 1 — ANALYSE PRÉLIMINAIRE DES RISQUES « SYSTÈME » ET DÉFINITION DES EXIGENCES ET DES CONTRAINTES « SYSTÈME »

Lors d'une évaluation de la sécurité, une analyse préliminaire des risques et des dangers et effectuée à un niveau « système » afin de définir les exigences en matière de sécurité ainsi que les contraintes en sécurité à intégrer. Cette analyse doit être la plus précoce possible dans le cycle de vie du système.

L'analyse préliminaire des risques « système » dans le système Novosol® est effectuée selon deux niveaux d'analyse : le premier niveau concerne le procédé technique Novosol® tandis que le second se focalise sur le système socio-technique Novosol®. Ce choix répond aux exigences du groupe Solvay et à la démarche méthodologique de la technique d'analyse des dangers STPA.

Ainsi, une première approche a été entreprise afin de fournir une réponse aux demandes industrielles en matière de gestion des risques au sein du système Novosol®. Ces demandes concernent l'évaluation des risques lors de la phase de phosphatation du système technique Novosol®.

Une évaluation des risques professionnels et une analyse HAZOP[20] ont été réalisées pour le procédé Novosol®. La méthodologie HAZOP se révèle en effet appropriée au procédé physico-chimique qu'est Novosol® [Ericson, 2005] ; soulignons d'ailleurs que, comme la technique STPA, la méthodologie HAZOP recherche d'éventuels écarts entre un état désiré du système et un état réel. L'HAZOP se focalise sur des paramètres techniques dans un système technique alors que STPA traite de problèmes de contrôle dans un système socio-technique en considérant les facteurs humain et organisationnel.

De plus, cette démarche centrée sur une HAZOP permet de caractériser les premières contraintes de sécurité pour la phase de phosphatation du procédé Novosol® centrées sur l'ingénierie du procédé. Pour sa mise en œuvre, l'HAZOP a été divisée en cinq étapes (figure 29) :

- une division du procédé par unité opérationnelle (zones de responsabilité de chaque opérateur) (*v.* figures 21 et 23). Pour mémoire, l'opérateur A est en charge du dégrillage, du stockage, du pompage et de la phosphatation des sédiments, de la mesure de la masse volumique des sédiments et du traitement des gaz ; l'opérateur B est en charge de la gestion des sédiments phosphatés et des bassins de stockage des liquides. L'opérateur C est quant à lui en charge des utilités, du chargement des camions et de la logistique d'approvisionnement et d'expédition ;
- une division de chaque unité opérationnelle en « moments » opérationnels (avant la mise en route, au démarrage, en fonctionnement, mise à l'arrêt) ;
- une division de chaque « moment » opérationnel en tâches opérationnelles ;

20 HAZOP (*Hazard and Operability Analysis*) [Ericson, 2005] est une technique d'analyse des dangers cherchant à identifier les déviations au sein d'un système ou d'un processus, très souvent physique et/ou chimique.

- une analyse de chaque tâche opérationnelle et une identification des écarts grâce à une grille HAZOP (figure 30) ;
- la définition de recommandations et de contraintes pour le procédé technique Novosol®.

La figure 30 reproduit un extrait de feuille d'analyse HAZOP.

L'ensemble de ces analyses[21] a permis de formuler des recommandations de sécurité et permettant d'améliorer aussi bien la conception d'une future installation Novosol® que le niveau de sécurité avant la mise en pleine exploitation.

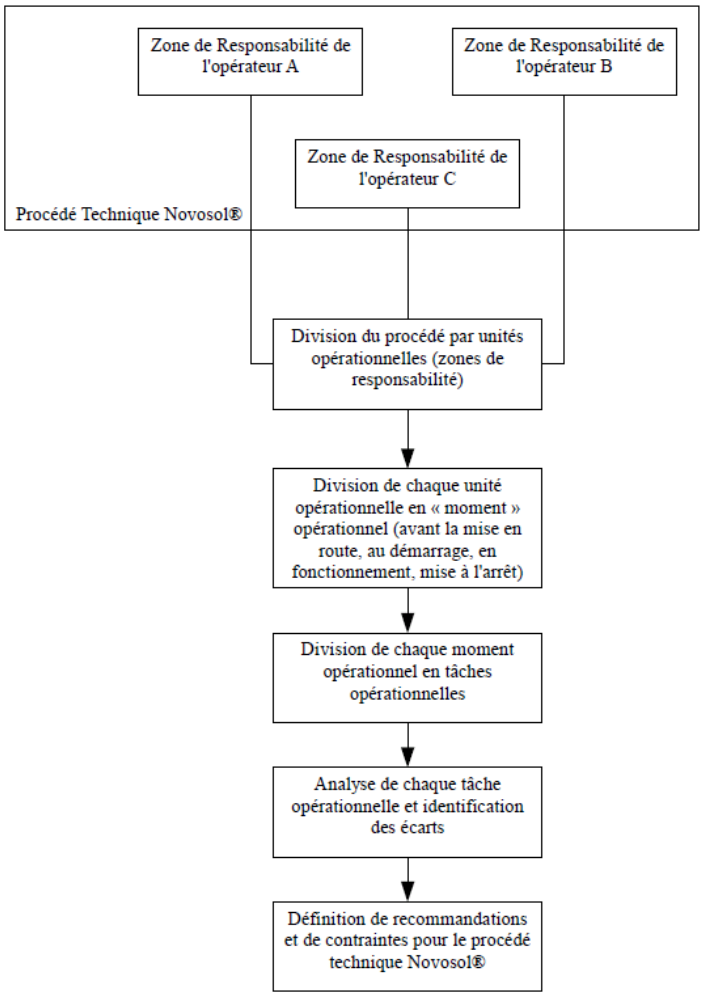


Figure 29 ■ Démarche HAZOP pour le procédé technique Novosol®

21 Rapports d'analyse livrés à Solvay courant 2009.

Unité	Tâche	Elément	Déviation	Paramètre	Mot Guide	Conséquence	Cause	Risque (classé suivant matrice des risques)	Contraintes
Unité Opérateur A avant mise en route	Tâche 2 : Contrôle de la teneur en eau des sédiments	Sédiments bruts	Contrôle inadéquate de la teneur en eau des sédiments	Siccité	Moins / Non	Teneur en eau trop importante Traitement non optimal des sédiments bruts lors de la phosphatation	Quantité en eau trop importante	3B	**Effectuer un contrôle systématique de la siccité pour chaque nouvelle barge**
					Trop	Teneur en eau trop faible	Quantité d'eau trop faible	3B	**Ajout d'eau (percolats) au niveau des trémies R01 et R03 pour diminuer la siccité**

Figure 30 ■ Extrait d'analyse HAZOP du système technique Novosol® et définition de recommandations et des contraintes de sécurité

Ces analyses ont permis de répondre aux exigences industrielles de Solvay mais ne correspondent pas à une démarche STPA, qui reste une technique nouvelle n'ayant jamais été appliquée dans le cadre d'un système tel que Novosol®. Elles sont par conséquent complétées par une seconde démarche et font l'objet d'une analyse plus globale. Le travail entamé par la suite ne s'intéresse pas exclusivement au système technique Novosol® mais au système socio-technique Novosol®, incluant aussi bien l'ensemble des facteurs humain et organisationnel du site que les entreprises de développement et d'exploitation Novosol®.

Pour chaque niveau hiérarchique du système étudié, les exigences et les contraintes « système » sont définies. Ainsi, pour l'entreprise exploitante du procédé Novosol® (Solvay lors des phases de développement de la technologie Novosol® et actuellement SEDISOL et SIFA) et dans le contexte actuel, les exigences et les contraintes selon la méthode STPA peuvent être établies comme indiqué dans le tableau 10.

Entreprise exploitante Novosol® (SEDISOL ou SIFA)
Contraintes et exigences de sécurité ■ Traiter des sédiments contaminés par des composés organiques et des métaux lourds. ■ Responsable du bon déroulement des inspections et de la constitution des rapports concernant l'exploitation et le développement Novosol® en liaison avec les entités nationales et internationales. ■ Responsable de la définition des exigences et des performances d'exploitation du procédé Novosol® au regard des réglementations nationales et internationales. ■ S'assure que les exigences d'exploitations soient bien intégrées et transmet tout évènement au niveau supérieur au regard des rapports reçus (exploitation et accidents).
Contexte dans lequel les décisions sont prises ■ L'écologie est un problème de société. ■ La pollution sédimentaire est un nouveau marché au regard de la demande des collectivités et des populations. ■ Procédé en cours de développement et en phase de prototypage. Nécessite donc une adaptation continue pour atteindre les performances exigées. ■ L'entreprise est en recherche ou en partenariat avec des futurs industriels potentiellement intéressés par la technologie Novosol®.
Actions de contrôle inadéquates (potentielles) ■ Dangers non identifiés. ■ Coordination inadéquate avec l'entreprise en charge du développement Novosol®. ■ Prise en compte inadéquate des rapports d'accident/incident. ■ Prise en compte inadéquate des rapports d'exploitation. ■ Intégration incomplète ou inadaptée des réglementations nationales et internationales. ■ Exigences de développement incorrectement définies au regard de la stratégie de l'entreprise exploitante.
Défauts du modèle cognitif ■ Penser que le procédé Novosol® développé est totalement sûr. ■ Ne pas avoir conscience de l'ensemble des risques lors de l'exploitation du procédé.

Tableau 10 ■ Exemple de définitions des exigences et contraintes pour le contrôleur : *Entreprise exploitante*

La définition de l'ensemble des exigences et contraintes pour les niveaux hiérarchiques ainsi définis permet l'établissement de la structure de contrôle hiérarchique.

► ÉTAPE 2 — ÉTABLISSEMENT DE LA STRUCTURE DE CONTRÔLE DE LA SÉCURITÉ (RÔLES ET RESPONSABILITÉS DES ÉLÉMENTS ET MÉCANISMES DE RÉTROACTION)

Cette deuxième étape permet la construction de la structure de contrôle de la sécurité du système à évaluer, incluant les rôles et les responsabilités de chaque élément (éléments de contrôle et rétroactions pour chacun de ces éléments).

La définition et l'établissement de la structure de contrôle de la sécurité des systèmes telle que développée par Nancy Leveson constituent la pierre angulaire de cette étape STPA [Leveson, 2004].

Chaque niveau ou élément de la structure de contrôle possède des rôles et des responsabilités visant à garantir que les contraintes en sécurité des systèmes sont appliquées au sein du système. La structure de contrôle de la sécurité ainsi définie, il est nécessaire de la modéliser.

La construction de cette structure passe par la mise en relation des différents niveaux hiérarchiques par le jeu des interactions entre les éléments. Cette étape s'appuie sur l'étape 1 en incluant l'ensemble des acteurs définis lors de l'établissement des exigences et des contraintes au sein du système Novosol®.

Cette étape permet d'obtenir une vision globale du système étudié, mais aussi de mettre en évidence l'ensemble des interactions entre les niveaux hiérarchiques du système. Par cette structure de contrôle, les rôles et les responsabilités sont intégrés et il est ainsi plus aisé de déterminer les influences entre éléments (figure 31). Cette structure décrit l'ensemble du système Novosol® d'un point de vue statique en montrant les rôles et les responsabilités de chaque niveau hiérarchique. Ces rôles et responsabilités servent de support à la définition et à l'intégration des contraintes au niveau de chaque acteur de la structure s'effectuant au cours de l'étape 3 de la méthodologie STPA.

La structure ainsi définie a pour objectif de représenter les interactions entre les différents niveaux hiérarchiques, permettant de caractériser les contrôles entre éléments. Ce travail de modélisation pose les limites de l'analyse afin de déterminer par la suite les contrôles potentiellement inadéquats entre niveaux.

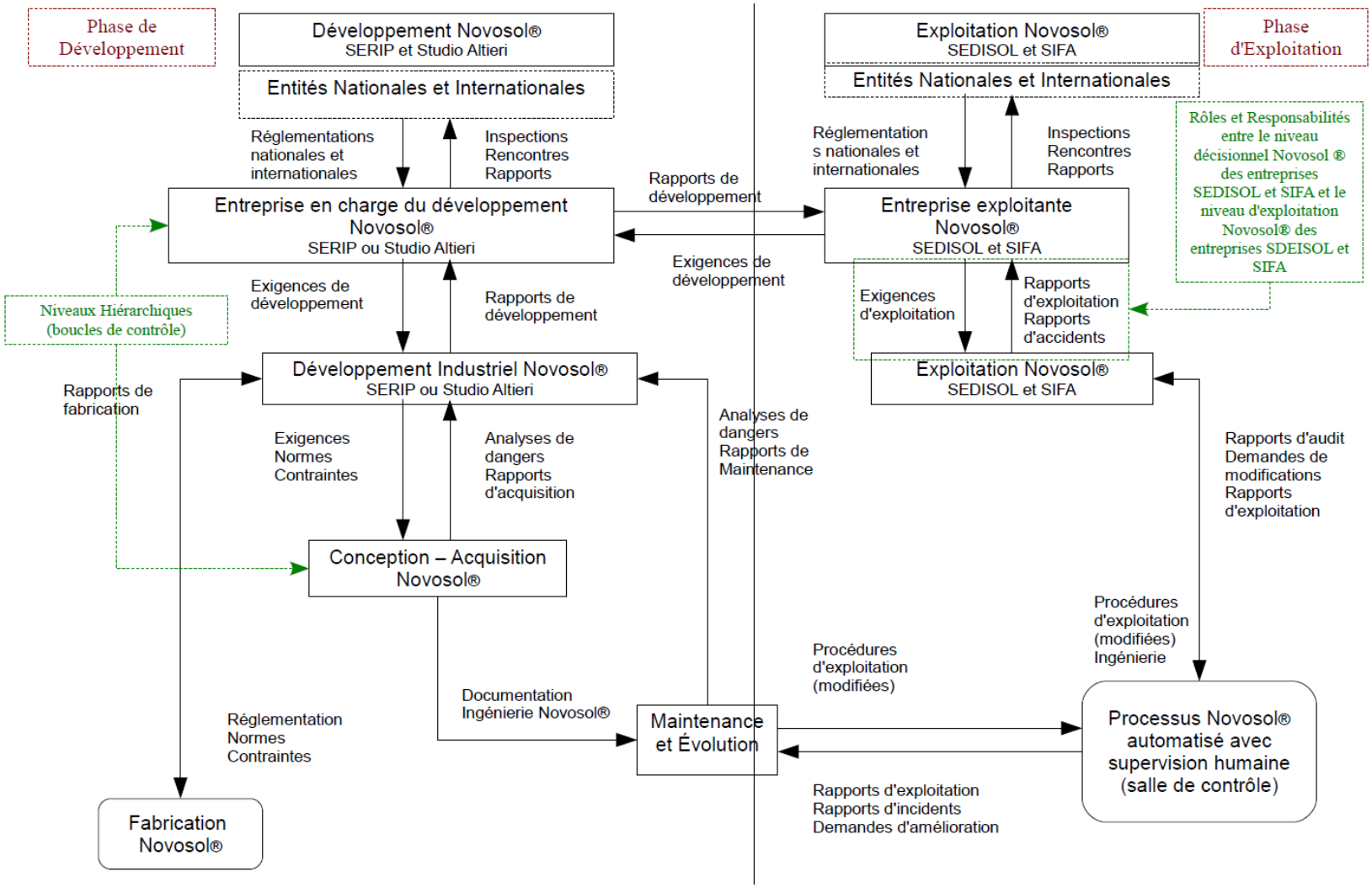


Figure 31 ■ Structure du système Novosol® lors de l'application de la technique d'analyse STPA.

► ÉTAPE 3 — INTÉGRATION DES EXIGENCES « SYSTÈME » ET DES CONTRAINTES « SYSTÈME » AU NIVEAU DES ÉLÉMENTS

L'intégration des exigences et des contraintes système définies lors de l'étape 1 doit s'effectuer au niveau de chaque niveau hiérarchique de la structure de contrôle de la sécurité définie lors de l'étape 2.

Cette troisième étape repose sur les deux précédentes, et vise à intégrer les exigences et les contraintes de sécurité au sein de chaque niveau hiérarchique. Ce travail s'effectue au regard des différentes interactions entre éléments. Cette étape permet la définition des exigences qui sont ensuite traduites sous forme de contraintes de sécurité au regard des différentes interactions entre les éléments de la structure de contrôle de la sécurité.

Un niveau hiérarchique supérieur — par exemple l'entreprise en charge du développement Novosol® (SERIP ou Studio Altieri) — définit des exigences de développement pour le niveau hiérarchique inférieur (développement industriel Novosol®). Ce niveau doit fournir une rétroaction (confirmation de contrôle) en faisant remonter les rapports de développement auprès du niveau supérieur (entreprise en charge du développement Novosol® : SERIP ou Studio Altieri). Il en est ainsi pour chaque interaction et chaque variable.

Concrètement à ce niveau de la structure, les sociétés SERIP ou Studio Altieri doivent définir et mettre en place des exigences de développement d'une installation Novosol® pour le service ou l'entité responsable du développement industriel. En retour, et afin que les directions de SERIP et de Studio Altieri soient informées de la bonne intégration de ces exigences de développement (de ces contrôles), le service ou l'unité fournit des rapports de développement décrivant les avancées du projet, voire les éventuelles difficultés rencontrées.

Ainsi, pour les niveaux hiérarchiques « entreprise en charge du développement Novosol® » et « développement industriel Novosol® », la formulation pourrait être la suivante : « L'entreprise en charge du développement Novosol® (SERIP ou Studio Altieri) doit définir des exigences de développement pour le niveau en charge du développement industriel Novosol® (SERIP ou Studio Altieri) ». En contrepartie, le niveau en charge du « développement industriel Novosol® (SERIP ou Studio Altieri) doit fournir des rapports de développement indiquant les avancées au niveau de « l'entreprise en charge du développement Novosol® (SERIP ou Studio Altieri) ».

► ÉTAPE 4 — EXAMEN DE LA STRUCTURE DE CONTRÔLE ET DES MODÈLES DE PROCESSUS POUR L'ANALYSE DÉTAILLÉE DES CONTRÔLES INADÉQUATS

Une analyse détaillée des contrôles inadéquats est requise lors de cette étape. Elle permet de définir les contrôles inadéquats potentiels susceptibles de jouer un rôle dans la survenance d'un accident.

Pour ce faire, cette analyse s'appuie sur quatre types de contrôles inadéquats :

- une action de contrôle potentielle n'est pas effectuée ;
- une action de contrôle potentiellement incorrecte ou non sûre est effectuée, menant à une perte ;
- une action de contrôle correcte est potentiellement effectuée trop tôt, trop tard, ou à un mauvais moment ;
- une action de contrôle correcte est potentiellement stoppée trop tôt.

Cette analyse se traduit par la définition d'actions de contrôle inadéquates (potentielles dans le cadre d'une démarche d'évaluation de la sécurité). Pour chaque niveau hiérarchique, les contrôles inadéquats sont définis conformément aux interactions établies lors de la construction de la structure de contrôle (tableau 11).

Entreprise exploitante Novosol® (SEDISOL ou SIFA)
Les actions de contrôle inadéquates (potentielles)
– L'entreprise exploitante ne fournit pas d'exigences d'exploitation au niveau de l'exploitation Novosol pour une exploitation sûre
– L'entreprise exploitante ne fournit pas d'exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante ne fournit pas de rapports d'inspection aux entités de contrôle
– L'entreprise exploitante fournit des mauvaises exigences d'exploitation à l'exploitation Novosol
– L'entreprise exploitante fournit des mauvaises exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante fournit des mauvais rapports d'inspection aux entités de contrôle
– L'entreprise exploitante fournit des exigences d'exploitation essentielles tardivement à l'exploitation Novosol
– L'entreprise exploitante fournit des exigences de développement essentielles tardivement à l'entreprise en charge de développement Novosol
– L'entreprise exploitante fournit des rapports d'inspection trop tardivement aux entités de contrôle
– L'entreprise exploitante ne fournit pas la totalité des exigences d'exploitation à l'exploitation Novosol
– L'entreprise exploitante ne fournit pas la totalité des exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante ne fournit pas la totalité des rapports d'inspection aux entités de contrôle

Tableau 11 ■ Actions de contrôles inadéquates pour le contrôleur : *Entreprise exploitante Novosol®*

L'ensemble de ces contrôles inadéquats est « traduit » en contraintes et en exigences de sécurité devant être intégrées au niveau de chaque élément du système.

Cette « traduction » s'effectue à partir des actions de contrôle inadéquates potentielles et des défauts de contrôle permettant d'inventorier les défauts et les dangers pouvant mener le système vers l'accident. Cette liste permettra de définir les contraintes que chaque niveau hiérarchiques se doit de respecter afin de maintenir un niveau de sécurité acceptable (tableau 12). Ces actions de contrôle inadéquates et

ces contraintes sont qualifiées de « potentielles » car elles sont supposées exister et ne sont définies que dans le cadre d'une évaluation de la sécurité.

Entreprise exploitante Novosol® (SEDISOL ou SIFA)
Les contraintes (potentielles)
– L'entreprise exploitante doit fournir des exigences d'exploitation à l'exploitation Novosol pour une exploitation sûre
– L'entreprise exploitante doit fournir des exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante doit fournir des rapports d'inspection aux entités de contrôle
– L'entreprise exploitante ne doit pas fournir de mauvaises exigences d'exploitation à l'entreprise Novosol
– L'entreprise exploitante ne doit pas fournir de mauvaises exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante ne doit pas fournir de mauvais rapports d'inspection aux entités de contrôle
– L'entreprise exploitante ne doit pas fournir des exigences d'exploitation tardives à l'exploitation Novosol
– L'entreprise exploitante ne doit pas fournir des exigences de développement tardives à l'entreprise en charge du développement Novosol
– L'entreprise exploitante ne doit pas fournir des rapports d'inspection tardivement aux entités de contrôle
– L'entreprise exploitante doit fournir la totalité des exigences d'exploitation à l'exploitation Novosol
– L'entreprise exploitante doit fournir la totalité des exigences de développement à l'entreprise en charge du développement Novosol
– L'entreprise exploitante doit fournir la totalité des rapports d'inspection aux entités de contrôle

Tableau 12 ■ Contraintes (potentielles) pour le contrôleur : *Entreprise exploitante Novosol®*

► ÉTAPE 5 — CATÉGORISATION (IMMÉDIAT, LONG TERME, STANDARD) ET « GESTION DES RISQUES » (DÉFAUTS DE BOUCLES DE CONTRÔLE)

Dans un premier temps, les risques identifiés sont catégorisés afin de déterminer l'incidence d'actions de contrôle inadéquates sur le comportement d'un système.

Dans un second temps, la gestion des risques est mise en œuvre par la détermination du ou des processus menant à la violation d'une ou de plusieurs contraintes de sécurité.

Cette dernière étape permet de hiérarchiser les priorités dans l'analyse des défauts de contrôle. Elle vise à optimiser le niveau de sécurité du système en traitant les risques immédiats considérés comme pouvant faire migrer le système vers l'accident dans un délai très court puis les risques à long terme (c'est-à-dire pouvant mener à l'accident après un délai important) et enfin les risques dits « standard » traités par une démarche en gestion de risques au cours du cycle de vie du système.

L'enjeu ici est d'identifier les contraintes à appliquer en priorité. Cette identification effectuée, il est ensuite nécessaire d'identifier à quel endroit d'une boucle de contrôle une contrainte de sécurité peut être violée (figures 32 et 33). À

chaque niveau de la boucle et à chaque interaction entre niveaux de la boucle, des contrôles inadéquats peuvent avoir lieu. L'objectif est ici, pour chaque niveau hiérarchique, d'identifier les contrôles inadéquats pouvant faire migrer le système vers un état accidentel. Chacun de ces contrôles au cours de la boucle peut avoir pour conséquence, en sortie, la formulation d'un contrôle inadéquat sur un autre niveau, entraînant ainsi une migration du système.

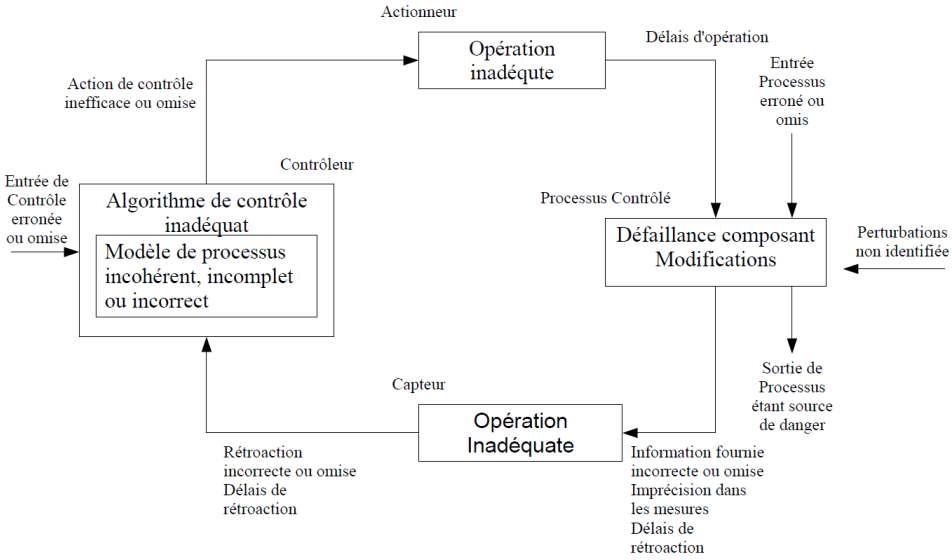


Figure 32 ■ Boucle de contrôle inadéquat
adapté de Leveson, 2010
Types d'actions au sein de la boucle de contrôle pouvant menant à un contrôle inadéquat. Ces actions potentielles doivent être identifiées afin d'éviter que le niveau hiérarchique ne fournisse un contrôle inadéquat.

À titre d'illustration, pour le niveau « Maintenance Évolution », la boucle de contrôle insérée peut être décrite de façon simplifiée (figure 33), c'est-à-dire sans établir de contrôles inadéquats potentiels au sein de la boucle de contrôle. Cette boucle (et chaque boucle de la structure de contrôle) fait partie du système Novosol® et il est alors essentiel de les analyser au regard de la totalité du système (figure 34) afin de déterminer la source de contrôles inadéquats potentiels.

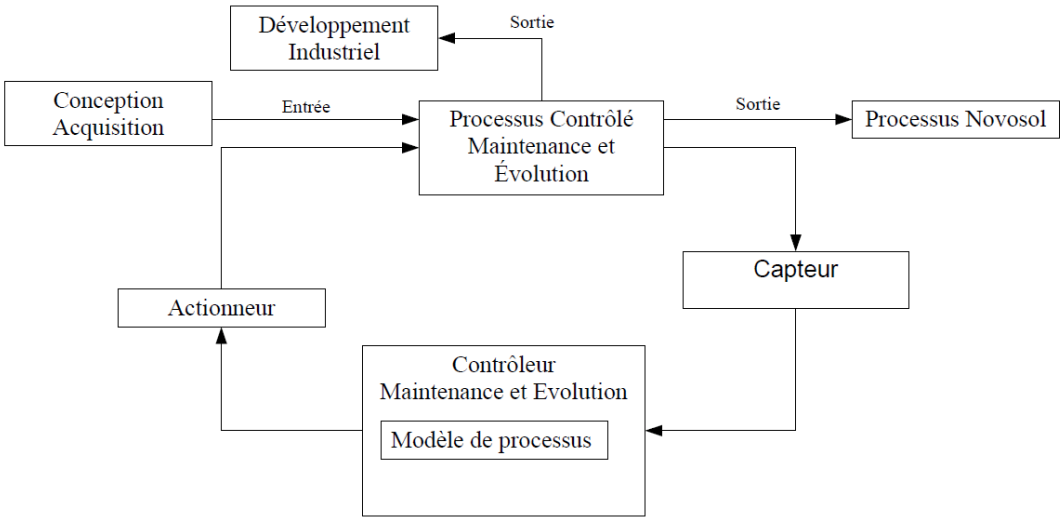


Figure 33 ■ Boucle de contrôle « Maintenance et Évolution »

Boucle de contrôle du niveau Maintenance et Évolution mettant en évidence l'ensemble des éléments impliqués dans le processus de contrôle de ce niveau en interaction avec les niveaux Développement industriel » et Conception Acquisition.
En se fondant sur la figure 32, cette boucle de contrôle pourrait contenir une information incorrecte en son sein qui provoquerait un contrôle inadéquat en sortie vers les niveaux Conception Acquisition et Développement industriel.

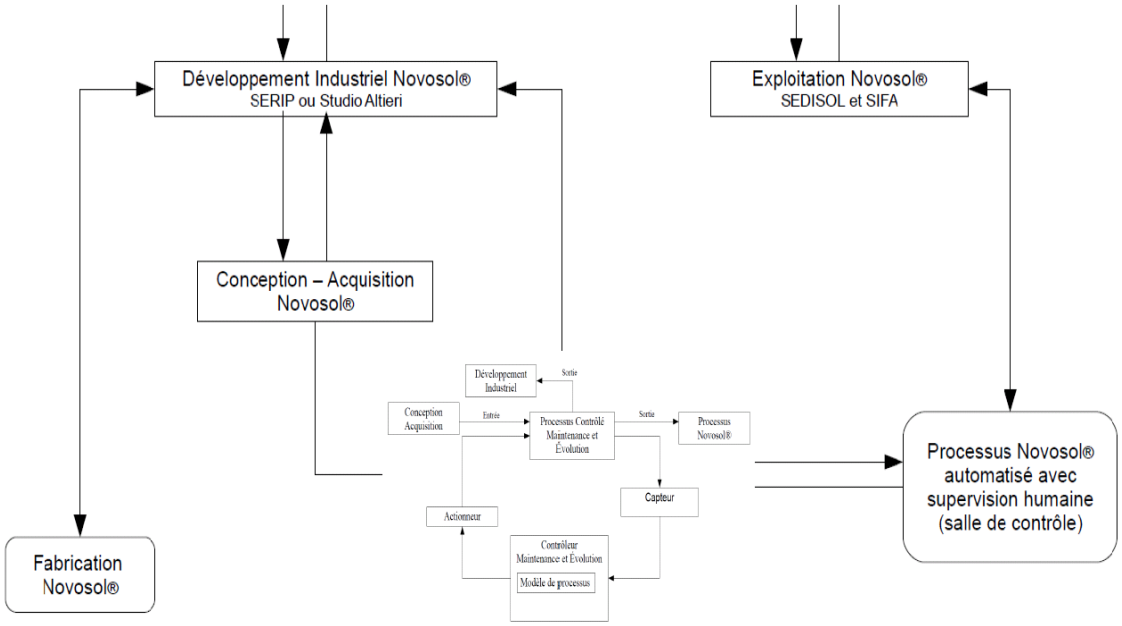


Figure 34 ■ Description d'une boucle de contrôle au sein de la structure de contrôle du système Novosol®

Intégration de cette boucle de contrôle au sein de la structure de contrôle permettant d'illustrer cette boucle de contrôle pour un niveau hiérarchique donné en interaction avec le reste de la structure de contrôle.

Cette phase de gestion des risques débute lors du développement d'une installation Novosol® par l'analyse des boucles de contrôle existantes.

Conclusion

Ce chapitre a été organisé selon de trois sections.

La première a présenté le contexte industriel dans lequel l'analyse des dangers STPA a été appliquée. Les sédiments contaminés constituent un problème environnemental non négligeable avec des impacts aussi bien économiques que sanitaires ou environnementaux. Pour répondre à cette problématique, plusieurs techniques de traitement des sédiments contaminés existent et ont été décrites.

Dans une deuxième, le système Novosol® a été décrit au sein de deux sous-sections. Une première sous-section a permis de présenter le procédé technique Novosol® divisé en deux étapes : une étape de phosphatation suivie d'une étape de calcination. Une seconde sous-section a été consacrée au système socio-technique Novosol® considérant l'ensemble des acteurs et des intervenants lors d'une démarche de traitement des sédiments contaminés.

Enfin, une dernière section a introduit les résultats de l'application de la technique d'analyse des dangers STPA au sein du système Novosol®. Les exigences formulées par l'industriel en charge du système Novosol® ont été remplies par l'application de techniques « traditionnelles ». Les résultats faisant suite à l'application de la technique STPA vise le système Novosol® dans sa globalité en prenant en compte l'ensemble des acteurs définis au sein d'une structure hiérarchique et ne se focalise pas uniquement sur un système « technique » comme cela peut être le cas pour des techniques d'analyse des dangers fondées sur des modèles d'accident traditionnels.

Chapitre 5
Perspectives d'évolution des modèles d'accident

Ce dernier chapitre a pour ambition de prendre du recul par rapport aux travaux précédemment conduits.

Il est construit autour de trois sections.

Une première section est consacrée à l'étude de la technique d'analyse des dangers STPA, fondée sur le modèle STAMP, d'un point de vue méthodologique. Cette section permet de classer la technique d'analyse STPA comme une technique en sécurité des systèmes et d'en apprécier les apports et les limites.

Une deuxième section traite des fondements théoriques du modèle d'accident systémique STAMP. Cette analyse a pour but de déterminer les principaux apports et limites d'un modèle d'accident systémique dans le cadre d'un système socio-technique.

Enfin, au regard des limites identifiées et du cadre scientifique actuel des modèles d'accident systémiques, une dernière section propose un changement de paradigme dans la compréhension des accidents au sein des systèmes socio-techniques. Ce nouveau paradigme, fondé sur la théorie du chaos, ne voit pas l'accident socio-technique comme un état provoquant systématiquement des pertes humaines ou matérielles, dû à un manque de contrôles, mais comme un évènement irréversible et imprédictible dû une absence de réponse adaptée faisant suite à une réorganisation non contrôlée dans un contexte donné et pouvant mener à des dommages et des pertes.

1. Les apports et limites de la technique STPA

Cette section est organisée en deux sous-sections : la première permet de classer la technique STPA comme une nouvelle technique en sécurité des systèmes ; la seconde présente les principales limites des outils de représentation et de modélisation lors de l'application de la technique STPA.

1.1. STPA : une technique en sécurité des systèmes

Cette section permet de préciser les apports et les limites de la technique d'analyse des dangers STPA.

L'analyse de la sécurité dans un système complexe regroupe un ensemble de concepts sur lesquels se fondent les spécialistes en sécurité des systèmes [DoD, 2000]. Ces concepts peuvent être énumérés [Benner, 1981] et ressortissent principalement ici du domaine industriel, tels qu'ils ont pu se développer dans le domaine de la sécurité des systèmes aux États-Unis à partir des années quarante :

- Sûr du premier coup ;
- Pour atteindre des niveaux de sécurité adéquats, il est nécessaire d'établir une démarche solide ;
- Prendre en compte le cycle de vie du système ;
- Fermer la boucle entre les attentes en sécurité et la performance ;
- Sélectionner le niveau de sécurité désiré dans le cadre d'une prise de décision réfléchie ;
- Utiliser des tests pour démontrer l'efficacité des mesures de sécurité ;
- Les enquêtes accident doivent fournir des améliorations durables sur le système ;
- La sécurité des systèmes prend en compte les interactions entre les hommes, les machines et l'environnement ;
- Les mesures de contrôle de la sécurité ont un ordre de priorité ;
- Les dangers les moins chers se trouvent dans les premières phases du cycle de vie du système ;
- La sécurité des systèmes a un rôle de facilitateur plutôt que d'obstacle dans l'atteinte des objectifs organisationnels ;
- La documentation des analyses de sécurité et des décisions est nécessaire dans un programme de sécurité pour une démarche rigoureuse et disciplinée ;
- La sécurité des systèmes exige des méthodes d'analyse de sécurité appliquées par des professionnels.

Ces concepts fondamentaux en sécurité des systèmes permettent de distinguer la sécurité des systèmes des autres approches ayant pour vocation la gestion des risques et des défaillances au sein des systèmes.

Pour intégrer ces concepts, la sécurité des systèmes utilise des techniques qui lui sont propres. Il est ainsi possible de se demander ce qui différencie une technique de

sécurité des systèmes d'une autre technique ou, plus simplement, ce qui fait d'une technique une technique de sécurité des systèmes.

La réponse à cette question permet de déterminer si une technique de sécurité est une technique de sécurité des systèmes plutôt qu'une technique d'ingénierie. Il semble donc légitime de se demander si la technique d'analyse des dangers STPA fondée sur le modèle d'accident STAMP est une technique de sécurité des systèmes. Il s'agit de vérifier si STPA répond aux critères de Benner présentés ci-après afin de confirmer que STPA est une technique d'analyse en sécurité des systèmes (tableau 13).

Dans sa démarche comme dans ses fondements, STPA peut être considérée comme une technique de sécurité des systèmes. Ses fondements systémiques, sa démarche centrée sur la sécurité d'un système, son processus d'application original et son organisation permettant l'application d'une démarche de sécurité répondent aux critères de Benner :

- STPA est-elle fondée sur la théorie des systèmes ? Ce critère cherche à déterminer si STPA se fonde sur les principes systémiques visant à analyser un système dans sa globalité et non en ayant recours à une approche analytique.
- STPA est-elle centrée sur la sécurité ? Ce critère cherche à déterminer si STPA remplit les exigences en matière d'analyse de sécurité.
- STPA est-elle fondée sur des connaissances propres ? Ce critère cherche à déterminer si elle a été développée à partir de connaissances uniques et non à partir de méthodes ou techniques déjà connues.
- STPA sert-elle à planifier une démarche sécurité ? Ce critère cherche à déterminer si STPA constitue une démarche d'analyse fondée sur une méthodologie déterminée en sécurité des systèmes tout au long du cycle de vie.

Aucune liste de critères officielle n'a été publiée mais certains permettent de reconnaître une authentique technique de sécurité des systèmes d'une autre et de déterminer si la technique d'analyse des dangers STPA est une technique de sécurité des systèmes.

Ces critères peuvent être de quatre ordres et se retrouvent dans toutes les démarches et analyses en sécurité des systèmes. Ainsi une technique d'analyse des dangers en sécurité des systèmes [Benner, 1981] :

- reflète les concepts généraux en théorie des systèmes :
  - elle prend en considération les grands principes systémiques, les entrées/sorties, les rétroactions…
  - elle ferme la boucle entre les performances attendues en sécurité et les performances d'exploitation ;
  - elle structure la recherche des données, l'organisation, les tests et l'analyse ;
- doit être centrée sur la sécurité plutôt que sur une autre discipline :
  - elle doit satisfaire les attentes en matière de sécurité ;
  - elle doit être applicable tout au long du cycle de vie du système ;

- doit permettre l'étude d'un corpus de connaissances, de concepts et de principes distincts de ceux rencontrés en sécurité des systèmes :
  - elle utilise un ensemble de concepts et de principes dans le domaine de la sécurité ;
  - son utilisation est différente de celles qui peuvent être faites dans d'autres disciplines ;
  - elle demande un suivi rigoureux des pratiques professionnelles afin de maintenir un niveau d'état de l'art à jour ;
- doit fournir une base pour établir des programmes et des plans de sécurité :
  - les techniques doivent faire partie d'un plan en sécurité des systèmes ;
  - les techniques produisent une documentation en analyse de sécurité qui assure de leur efficacité ;
  - les techniques fournissent un moyen de suivi d'exploitation et des accidents pour évaluer les niveaux de performance devant être atteints.

Fondée sur la théorie des systèmes ?			**Centrée sur la sécurité ?**		**Fondée sur des connaissances propres ?**			**Sert à planifier une démarche en sécurité ?**		
Prend en considération les principes systémiques	Fait le lien entre les performances attendues et d'exploitation	Structure la recherche des données d'analyse	Satisfait aux attentes en matière de sécurité	Est applicable tout au long du cycle de vie du système	Utilise un ensemble de connaissances dans le domaine de la sécurité	S'utilise de façon unique	Demande un suivi des pratiques professionnelles	Est intégrée dans une démarche sécurité	Fournit une documentation permettant un suivi d'analyse	Permet une analyse des accidents dans un souci de performance
Oui	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**
Technique d'analyse STPA basée sur le modèle STAMP										

Tableau 13 ■ Critères de Benner pour la technique STPA
adapté de Benner, 1981

La mise en œuvre de la technique STPA demande d'en comprendre les concepts et l'« esprit » ; en pratique, certaines étapes se révèlent délicates car elles dépendent fortement de l'analyste. Diverses améliorations doivent encore venir éclaircir certains des concepts de la méthode, et notamment sa taxonomie sur la classification des défauts de contrôle. La technique STPA est fondée sur le modèle STAMP, lui-même conçu sur le modèle de Rasmussen dans lequel des contrôles opèrent entre les différents niveaux hiérarchiques de sa structure [Rasmussen, 1997]. Ainsi, comprendre une telle organisation facilite l'application de la technique STPA aux différents éléments d'un système donné.

La technique STPA requiert une phase d'appropriation. En effet, une technique en sécurité des systèmes se focalise généralement sur l'identification, l'évaluation et la maîtrise des dangers et des risques associés. STPA n'est pas une démarche de recherche des dangers mais de recherche de contraintes pouvant mener le système vers un état accidentel. Par conséquent, un ingénieur en sécurité souhaitant s'approprier la technique STPA ne doit pas se polariser sur les dangers et les risques mais chercher, entre les niveaux hiérarchiques, les contrôles pouvant s'avérer inadéquats.

Les résultats d'une analyse STPA restent centrés sur des facteurs humain et organisationnel. STPA permet de formuler des recommandations visant à l'amélioration des contrôles entre niveaux hiérarchiques dont le but est d'éviter la migration du système vers un état accidentel. Elle permet d'optimiser le niveau de sécurité par une amélioration dans la définition des contraintes, de la structure et des boucles de contrôle du système étudié.

Les avantages de l'application de la technique STPA sont indéniables par rapport à une technique fondée sur un modèle d'accident traditionnel [Johnson, 2004]. STPA conduit par exemple à une amélioration des contrôles au niveau des interactions entre éléments et par conséquent, à une amélioration de la performance globale du système étudié. STPA permet également la prise en compte des changements au sein d'un système au cours du temps, dimension dynamique qu'aucune des approches traditionnelles ne revêt [Setiadi, 2006].

1.2. Les apports et les limites des outils de représentation systémique

Le système étudié dans le cadre de l'application d'une technique fondée sur le modèle d'accident STAMP peut être représenté grâce à des outils informatiques de modélisation et de simulation dynamique. Parmi eux, les logiciels Stella[22] et Vensim[23]

22 http://www.iseesystems.com/softwares/Education/StellaSoftware.aspx.

23 http://www.vensim.com/

sont parmi les plus utilisés par les laboratoires de recherche ou les entreprises engagés dans une démarche d'analyse d'un système dynamique. Ces logiciels exploitent des systèmes dynamiques définis par un ensemble de variables d'état (ou stocks) et un arsenal d'équations différentielles autour desquelles le logiciel est construit et qui permet de caractériser le mouvement du système étudié au cours du temps.

L'analyste doit quant à lui « poser » son système (ses variables d'état) dans un espace de travail dédié. Pour cela, il doit posséder une parfaite connaissance des éléments constituant le système étudié ainsi que les interactions entre ses composants. Le comportement du système est résolu par une équation différentielle permettant de représenter sa « trajectoire ». Ce type de logiciel s'avère capable de résoudre des équations différentielles intégrables, c'est-à-dire de représenter un comportement d'un système dynamiquement linéaire.

Ces logiciels sont extrêmement efficaces dans l'analyse et dans la prédiction des comportements dynamiques de systèmes techniques, dont le comportement est à la fois déterministe, intégrable et prédictible. Par conséquent, toute analyse d'accident ou d'évaluation de la sécurité dans le cadre d'un système technique peut être effectuée en utilisant un modèle d'accident systémique adéquat tel que le modèle STAMP.

Cependant, ces logiciels montrent leurs limites dans leur capacité à prédire le comportement d'un système socio-technique. Un système socio-technique est un système complexe possédant des interactions non linéaires. Son comportement se traduit par des équations différentielles non linéaires qui ne peuvent être résolues que dans des cas très particuliers. En pratique, des logiciels tels que Stella ou Vensim, fondés sur la résolution d'équations différentielles linéaires, ne peuvent prédire le comportement d'un système socio-technique. Par conséquent, il demeure à ce jour impossible de modéliser et de simuler de façon parfaite le comportement d'un système socio-technique à l'aide de ces outils.

Face à ce problème d'analyse des systèmes dynamiques non linéaires, une réponse est partiellement apportée par des démarches mathématiques de « linéarisation ». Le but est, à partir d'un système dynamique au comportement non linéaire, d'obtenir des équations différentielles linéaires d'un comportement. Ces équations obtenues sont par conséquent intégrables et il est donc possible d'y trouver une solution potentielle (loi d'évolution) permettant une prédiction.

2. Les apports et les limites du modèle d'accident STAMP

Cette section s'attache à présenter les principaux apports et les limites du modèle d'accident systémique STAMP. C'est pourquoi elle examine dans un premier temps

les prérequis nécessaires à la mise en œuvre d'un modèle d'accident systémique au regard des insuffisances des modèles d'accident traditionnels, puis les limites du cadre théorique de ce type de modèle à traiter les systèmes complexes, par essence instables.

2.1. Les prérequis à la mise en œuvre des modèles d'accident systémiques

Les modèles d'accident systémiques sont fondés sur la théorie générale des systèmes et la théorie du contrôle. Ils sont caractérisés par un aspect dynamique et un aspect hiérarchique (selon l'approche de Rasmussen) [Rasmussen, 1997]. Au delà de la maîtrise des théories des systèmes et du contrôle, un modèle d'accident systémique implique la pleine possession des modèles d'accident dits traditionnels. Ces modèles demandent à l'analyste une formation en sécurité des systèmes, passant par une connaissance des approches et des techniques appliquées à ce champ disciplinaire.

L'application d'un modèle d'accident systémique demande d'acquérir des connaissances préalables au sein des théories du contrôle et des systèmes. Ainsi, les concepts de systémique, de contrôle, de boucle de contrôle, de rétroaction (feedback), etc. doivent être parfaitement connus, ce qui impose dans les faits une maîtrise de concepts appartenant aussi bien au domaine « systémique » qu'au domaine de la sécurité. Ces modèles demandent à l'analyste d'acquérir une vision globale orientée « sécurité » afin d'étudier ou d'analyser un système dans sa globalité. Par ailleurs, l'évolution des modèles d'accident pousse à maîtriser de nouvelles disciplines telles que la dynamique de systèmes ou les applications informatiques de modélisation de systèmes dynamiques.

Dans le domaine de la systémique, l'utilisation d'un modèle d'accident systémique requiert une maîtrise des «fondements » de la pensée système :

- qu'est-ce qu'un système ? comment l'appréhender ?
- qu'est-ce que la complexité ?
- quels sont les différents types de systèmes ?
- qu'est ce qu'un système dynamique ? qu'est ce qu'une rétroaction ?
- qu'est-ce qu'un comportement dynamique ?...

L'utilisation d'un modèle d'accident systémique conduit à maîtriser les concepts spécifiques à la sécurité des systèmes :

- qu'est-ce que la sécurité ? qu'est-ce qu'un processus en sécurité des systèmes ?
- qu'est-ce qu'une technique d'analyse des dangers ?
- comment intégrer une technique d'analyse dans le cycle de vie d'un système ?
- qu'est-ce qu'un danger ? qu'est-ce qu'un accident ?
- quel est le triptyque d'une démarche d'analyse des dangers ?...

La parfaite maîtrise de l'ensemble de ces domaines et concepts s'impose à tout analyste, choisissant d'opérer par l'application d'un modèle d'accident systémique. Un temps d'adaptation et de formation est par conséquent nécessaire avant d'appliquer une telle approche à un système socio-technique.

Toutefois, une bonne connaissance des domaines de la sécurité et de la systémique n'est pas suffisante pour exploiter des modèles d'accident systémiques : ces derniers demandent à leur utilisateur une compréhension intime de leurs enjeux, qui va bien au delà d'une application de principes sécuritaires au sein d'un système donné. Il s'agit bien plutôt de comprendre un système dont la sécurité est une propriété émergente, et donc de mettre en évidence une complémentarité entre un niveau de sécurité et une optimisation systémique.

2.2. Les apports et les limites des cadres théorique et scientifique des modèles d'accident systémiques

Les apports des modèles d'accident systémiques constituent aussi, paradoxalement, leurs limites. Ces apports (et ces limites) sont doubles. Les modèles d'accident systémiques, se fondant sur la théorie générale des systèmes et la théorie du contrôle permettent une meilleure prise en compte des notions d'équilibre et de temps.

Une première approche expose les apports de ces modèles dans la prise en compte de l'aspect non linéaire du comportement des systèmes socio-techniques dans la recherche de leur équilibre. Elle considère également la prise en compte de l'aspect dynamique permettant d'intégrer les notions de temps et d'évolution au cours des analyses.

Une seconde étape traite des limites des modèles systémiques se focalisant sur les notions d'équilibre et de temps. Elle conteste l'opportunité d'étudier un système socio-technique lorsqu'il se trouve dans un état d'équilibre stable comme le suggère la théorie générale des systèmes. Par ailleurs, elle reconsidère la prise en compte de la notion de temps au travers de la notion de « flèche du temps ».

2.2.1. Les apports des modèles d'accident systémiques

Les modèles d'accident systémiques pallient les limites des modèles d'accident traditionnels fondés sur l'approche analytique, inadéquate face à des systèmes dynamiques. Les premiers modèles d'accident dits linéaires n'étaient capables de fournir que des solutions « stables » et prédire des situations d'instabilité de quatre types :

- des situations d'oscillations stables, c'est-à-dire des variations faibles du système, équilibrées grâce à des réponses linéaires et proportionnées ;

- des situations d'oscillations de croissance exponentielle, c'est-à-dire un comportement systémique caractérisé par des boucles de rétroaction positives et expansives et des boucles négatives permettant « d'amortir » la variation ;
- des situations de stabilité asymptotique, caractérisées par des boucles de rétroaction négative permettant d'atteindre un objectif ou de stabiliser un système ;
- des situations de croissance sans limite, caractérisées par des boucles de rétroaction positives engendrant un phénomène de croissance exponentielle.

Un des avantages des modèles d'accident linéaires est leur capacité à fournir des prédictions précises concernant l'état futur d'un système alors que des modèles d'accident systémiques ne fournissent qu'une (loi d') évolution d'un système. Or, la dynamique des systèmes et celle des systèmes socio-techniques ne sont pas linéaires. Pour comprendre un système « accident » dans le cadre d'un modèle d'accident linéaire, il suffit de modéliser un système en examinant son comportement lorsqu'il est à l'état d'équilibre. Une fois cette modélisation effectuée, il est alors possible de prédire le comportement général du système lorsque les conditions initiales sont connues. Cependant, ces modèles d'accident linéaires ne sont valables et réellement adaptés que lorsque le système se trouve dans une situation proche d'un état d'équilibre stable.

Les modèles d'accident systémiques, fondés sur la théorie générale des systèmes et sur la théorie du contrôle, se focalisent sur l'analyse d'un système en état d'équilibre stable évoluant vers un état accidentel. Dès lors que les informations concernant les éléments du système sont connues, il devient possible de décrire son comportement dynamique, de l'analyser ou de mener une enquête accident. Autrement dit, dès que les conditions initiales d'un système dynamique sont connues, il est possible de décrire sa trajectoire et sa loi d'évolution.

Les modèles d'accident systémiques sont ainsi capables de produire des types de solutions autres que ceux décrits par les modèles d'accident traditionnels tout en permettant des changements structurels. Ils permettent également de proposer des pistes afin de renforcer la robustesse d'un système, c'est-à-dire sa sensibilité à de petites perturbations afin de le maintenir dans un état « sûr ».

Dans ce cadre, un modèle d'accident systémique tel que le modèle STAMP cherche à renforcer la robustesse et la stabilité d'un système face à des perturbations. Deux types de stabilité existent dans un système dynamique : une stabilité dynamique et une stabilité structurelle. La stabilité dynamique se traduit par un comportement du système face à une perturbation extérieure au système (par exemple un « bruit » externe au système). Dans ce cadre, le système va chercher à fournir une réponse adapté à un signal extérieur tout en préservant un état « sûr ». La stabilité structurelle (qui est au cœur du modèle STAMP avec l'établissement et l'étude d'une structure hiérarchique) concerne le contrôle de la structure (composée d'un grand nombre d'éléments en interactions non linéaires). Cette stabilité structurelle reste

interne au système et le maintien d'un état « sûr » dépend de la capacité du système à maintenir un contrôle interne sur sa structure.

Les modèles d'accident systémiques ont donc été développés afin de prendre en considération la complexité au sein des systèmes socio-techniques. Dans de nombreuses références bibliographiques, la complexité est synonyme d'un nombre important d'interactions entre les éléments. Cette condition est nécessaire mais pas suffisante. En effet, un système peut être composé d'un grand nombre d'interactions sans qu'aucune complexité ne soit caractérisée (par exemple, un glaçon, composé de très nombreuses molécules en interaction linéaire se trouve dans un état d'équilibre stable). La condition supplémentaire pour caractériser la complexité est la notion de non-linéarité. Un système composé de nombreux éléments en interactions non linéaires sera alors considéré comme un système complexe. Tel est le cas des systèmes socio-techniques.

Les modèles d'accident systémiques reposent sur la théorie générale des systèmes de Bertalanffy. Dans ce cadre, ils étudient des systèmes en état d'équilibre stable ou proche de cet état d'équilibre stable (lorsqu'ils subissent des perturbations). Or, des systèmes complexes ne sont jamais en état d'équilibre stable et il est donc inadapté de vouloir les étudier comme des systèmes complexes avec des outils fondés sur une théorie étudiant des systèmes en état d'équilibre stable ou proche de cet état.

Cette contradiction est sous-jacente au modèle d'accident STAMP.

2.2.2. Les limites des modèles d'accident systémiques

Le modèle d'accident STAMP est fondé sur deux théories que sont la théorie des systèmes de Ludwig von Bertalanffy [Bertalanffy, 1968] et la théorie du contrôle avec notamment les travaux de Norbert Weiner sur le concept de rétroaction. Ces théories ont posé les caractéristiques des systèmes décrits dans le cadre de la science classique. Il s'agit de la notion d'équilibre, de causalité linéaire et de rétroaction négative. Ces notions permettent d'expliquer dans quel cadre les modèles d'accident se sont développés.

La notion d'équilibre correspond à l'état d'un système lorsqu'il corrige automatiquement des déviations de trajectoire déterminées par des lois basiques. Dans ce cadre, un système socio-technique est un ensemble de systèmes pour lequel l'état naturel est un système en état d'équilibre stable où toute déviation est atténuée ou corrigée grâce à des rétroactions négatives. Lorsqu'une perturbation est trop importante et ne permet pas le retour à l'état initial d'équilibre, le système peut migrer vers un nouvel état d'équilibre.

La causalité linéaire postule qu'il existe un lien direct entre la cause agissant sur un système et dans les changements de la structure du système, c'est-à-dire une proportionnalité entre la cause et l'effet.

Enfin, la rétroaction négative, présente dans les recherches de Newton [Newton, 1687], Darwin [Darwin, 1859] ou Bertalanffy [Bertalanffy, 1968], traduit un mécanisme existant lorsqu'un système s'éloigne de l'équilibre en raison de perturbations externes ou de fluctuations inhérentes à sa dynamique qui atténue les effets de celles-ci pour permettre au système de revenir vers son état d'équilibre initial. La notion de rétroaction négative a largement inspiré le domaine de la cybernétique.

Les modèles d'accident sont développés afin de décrire, interpréter et prédire un accident. La démarche du modèle d'accident exploitée ici reste une démarche déterministe constituant le principe fondamental de toute prédiction. En effet, l'objectif fondamental d'un modèle d'accident est d'ordre prédictif en s'attachant à l'analyse des dangers dans un système (statique ou dynamique, linéaire ou non linéaire) afin de prévenir des comportements pouvant faire migrer un système « sûr » vers un état accidentel. L'ensemble des modèles d'accident ont été conçus dans un souci de compréhension et de prédiction au sein de différents types de systèmes tels que des systèmes physiques ou des systèmes socio-techniques. Les modèles d'accidents linéaires sont limités et ne représentent qu'une approximation de la réalité qui ne peut être acceptée que lorsque le système est proche d'un état d'équilibre stable. Or, un phénomène accidentel ne se déroule jamais quand un système est proche d'un état d'équilibre stable. Ces modèles d'accident se sont construits sur une démarche déterministe, alliant approche analytique et approche systémique (désormais considérées comme complémentaires [De Rosnay, 1995]). Ces modèles d'accident ont toujours supposé que les systèmes étudiés étaient des systèmes déterministes « intégrables » (linéaires). Cependant, des systèmes tels que des systèmes socio-techniques intègrent de nombreux éléments en interaction non linéaire, générant de nombreux types de comportements et donc d'évolutions.

Une conséquence est, dans les modèles d'accident systémiques, la prise en compte de la notion de « temps ». À l'heure actuelle, la modélisation des systèmes socio-techniques est fondée sur la théorie des systèmes dynamiques intégrables, c'est-à-dire des systèmes proche d'un état d'équilibre stable dans lesquels le temps s'écoule de façon continue et perpétuelle. Dans ces modèles d'accident systémiques, le système est dynamique et évolue donc au cours du temps. Or, un modèle d'accident systémique étudiant un système dynamique en état d'équilibre stable ne peut pas être amené à évoluer de façon continue du fait de réponses uniquement « linéaires » face à des perturbations. Un système, quel qu'il soit, se trouvant en état d'équilibre stable ne peut évoluer car sa trajectoire est un point fixe ne se trouvant pas en mouvement. Un état d'équilibre stable n'est régi que par des processus linéaires et ne pousse pas le système à changer. Un système n'évolue que dans l'instabilité par le biais de processus irréversibles. Il devient alors difficile de parler de dynamique et d'évolution au cours du temps, comme ceux définis dans le cadre de la théorie générale des systèmes de Bertalanffy, dans le cadre de systèmes en état d'équilibre instables, comme le sont les systèmes socio-techniques.

Le temps est un paramètre qui s'impose à tout système. Il doit être considéré comme un degré de liberté, voire comme une propriété émergente, et non comme un paramètre universel s'imposant par défaut à tout système. Les lois physiques sur lesquelles se fonde la théorie générale des systèmes ne font pas de distinction entre des directions future et passée d'une « flèche du temps » [Prigogine, 2001] au sein d'un système dynamique non intégrable. Or, cette notion de « flèche du temps » prend tout son sens dans la théorie des systèmes dynamiques non intégrables.

Ainsi, le temps (et notamment la « flèche de Temps ») émerge de l'instabilité et de l'irréversibilité des processus. L'entropie naît de l'irréversibilité, qui est inexistante dans un état d'équilibre stable. De l'instabilité et de la non-linéarité, émerge la « flèche du temps », source de phénomènes comme l'auto-organisation et l'évolution. Dans cette optique, les changements au sein d'un système socio-technique n'apparaissent pas au bout d'un temps donné mais lors de l'apparition de sa « flèche du temps » qui émerge de processus non linéaires au sein d'un système dynamique non-intégrable. Autrement dit, la notion de « flèche du temps » prend son « sens » dans les processus irréversibles.

Par conséquent, l'évolution même d'un système est sa capacité à faire émerger sa « flèche du temps » en passant par un état d'équilibre instable et donc de non-linéarité. Cette « flèche du temps » est créatrice et constitue une source de changement au sein de la structure même du système. Ainsi, cette flèche du temps n'existe que dans l'existence, c'est-à-dire uniquement dans l'apparition de processus irréversibles menant au changement et à l'évolution contrairement à une approche classique d'un « temps » apparu avant toute existence qui serait continue et perpétuelle.

L'évolution d'un système socio-technique ne dépend pas d'un facteur « temps » continu et perpétuel comme on pourrait le définir lors de l'utilisation d'un outil de modélisation fondé sur la théorie générale des systèmes de Bertalanffy. Un système socio-technique est générateur de sa propre « flèche du temps » caractérisée par des phénomènes non linéaires et irréversibles mettant en évidence une brisure de symétrie. Le temps ne prend son « sens » que parce qu'un système socio-technique est un système complexe. Ainsi, la stabilité (voire la sécurité) d'un système socio-technique peut être obtenue par une adaptation de sa structure dans un contexte donné, c'est-à-dire par des processus irréversibles en réponse à un contexte donné.

Les modèles d'accident systémiques considèrent le temps comme un paramètre n'ayant aucune influence sur le système étudié. Or, on vient de le voir, c'est dans l'émergence de cette « flèche du temps » dans un état fort éloigné de l'équilibre qu'un système peut construire sa propre structure tournée vers la sécurité.

3. Proposition d'un cadre théorique et conceptuel pour un premier modèle d'accident « chaotique »

Cette dernière section est organisée en deux sous-sections. La première décrit le cadre scientifique des systèmes non intégrables tels que les systèmes socio-techniques. Cette section vise à introduire brièvement la théorie du chaos. Une deuxième sous-section propose de considérer la théorie du chaos comme fondement pour l'établissement d'un nouveau modèle d'accident.

3.1. Un cadre déterministe non intégrable : la théorie du chaos

Il faut attendre les travaux d'Henri Poincaré [Poincaré, 1908] et sa théorie du chaos du début du XX^{e} siècle, puis l'arrivée de l'informatique pour remettre en cause la linéarité du déterminisme. Avant Poincaré, la notion d'équilibre était synonyme de vérité, d'ordre et de progrès et son contraire signifiait désordre, erreur et accident. Poincaré a eu pour ambition d'étudier des systèmes à « trois corps » en concluant que tout système déterministe n'est pas intégrable et donc que tous les systèmes déterministes ne sont pas prédictibles. Il s'intéresse non pas à un mouvement particulier mais à un flot dans l'espace des phases[24]. Ainsi, un système dynamique déterministe ayant au moins trois variables comprenant des termes non linéaires (dus à des rétroactions) peut présenter un comportement instable rendant ainsi toute prédiction impossible sur son évolution future. À partir de ce constat, il apparaît légitime de se demander si les modèles d'accident actuels, utilisés pour les systèmes socio-techniques, restent efficaces et performants au regard de la non-linéarité de systèmes à trois éléments en interaction et plus, menant *a fortiori* à un état d'instabilité.

Poincaré constate en effet qu'une très petite variation des conditions initiales d'une expérience peut entraîner des perturbations gigantesques, montrant ainsi une certaine dépendance sensitive aux conditions initiales d'un système comme il peut le préciser dans son ouvrage *Science et méthode*, publié en 1908 [Poincaré, 1908] : « une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard(…). Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit ». La « dépendance sensitive des conditions

24 L'espace des phases d'un système est un espace comportant d'un repère dont les axes de coordonnées correspondent aux degrés de liberté caractérisant le comportement du système. Ainsi, un point de cet espace des phases représente un état unique du système. L'évolution d'un système est donc une suite de points (une trajectoire) représentant ses différents états au cours du temps.

initiales » constitue donc un concept fondamental de la théorie du chaos. Appliquer cette caractéristique à des modèles d'accident (notamment systémiques) met en évidence les limites d'une démarche de prédiction et d'analyse dans la recherche et l'identification de dangers voire de comportements pouvant mener un système vers un état accidentel. En effet, un modèle n'a jamais eu pour objectif de représenter la réalité. Il s'attache principalement à résoudre un problème défini et reste donc, de par sa définition, prédictible sous certaines conditions. Ce constat implique également qu'en raison d'une dépendance sensitive aux conditions initiales, un modèle d'accident peut être à l'origine de comportements très divergents au bout d'un certain laps de temps, voire migrer vers un comportement chaotique ou avoir des trajectoires de phases différentes [Lurçat, 1999]. Par conséquent, dans les systèmes réels, le chaos empêche toute prédiction de l'évolution future après un certain temps en raison d'une précision insuffisante des mesures, même si le processus de contrôle du système est connu et peut être transformé en un modèle.

Les travaux de Poincaré et plus particulièrement ses travaux dans le domaine de la météorologie ont par la suite inspiré un autre météorologiste, Edward Lorenz. Ce dernier a pu observer le premier exemple connu de comportement chaotique lors d'une expérimentation durant laquelle, par souci de simplicité, il poursuivit une démonstration en tronquant certains résultats au millième au lieu du millionième. Il écrit en 1963 dans son article « Deterministic Non-Periodic Flow » : « *cela implique, dit-il, que deux états qui ne diffèrent que par d'infimes quantités peuvent évoluer vers deux états totalement différents. Partant de là, s'il y a la moindre erreur dans l'observation d'un état présent, et de telles erreurs semblent inévitables dans n'importe quel système réel, il se pourrait bien qu'il soit impossible de faire une prédiction valable de ce que deviendra cet état dans un futur lointain* » [Lorenz, 1963]. Dans son modèle, la forme que prennent les trajectoires représente un papillon. C'est lors de la 139e réunion de l'American Association for the Advancement of Science en 1972 qu'il nomme ce phénomène « l'effet papillon » [Lorenz, 1972] et voit l'apparition de la notion d'attracteur[25]. L'imprédictibilité serait ce phénomène qui pourrait être contrôlé par des attracteurs permettant de maintenir une stabilité relative tant que les perturbations ne sont pas trop importantes.

3.2. Vers l'émergence d'une nouvelle forme de modèle d'accident

Cette sous-section est organisée autour de quatre articulations. Une première articulation présente les notions d'instabilité et de résonance ; une deuxième

25 Un attracteur est un objet géométrique représentant le lieu de convergence de toutes les trajectoires des points de l'espace des phases, c'est-à-dire une situation ou un ensemble de situations vers lesquelles évoluent un systèmes, quelles que soient les conditions initiales. À cette notion d'attracteur est associée la notion de bassin d'attraction représentant l'ensemble des points de l'espace des phases menant à un attracteur.

articulation traite de la notion de bruit comme source de perturbation au sein d'un système ; une troisième pose les fondements d'un nouveau modèle d'accident ; enfin, une dernière articulation reprend le phénomène « accident » dans le cadre d'un nouveau modèle d'accident.

3.2.1. Instabilité et résonance

Un système dynamique est instable si son évolution est imprédictible car une petite variation de sa trajectoire peut prendre d'importantes valeurs. Sa trajectoire peut diverger de façon exponentielle et devient chaotique au bout d'un certain temps[26].

« L'analyse du chaos déterministe montre qu'à partir d'un point de départ déterministe se produisent toute une série de phénomènes et de réactions qu'on ne peut pas prédire parce qu'on ne peut pas connaître totalement les conditions initiales. Même lorsque vous avez un système déterministe, son comportement peut être chaotique » [Morin, 2002]. Ce chaos déterministe a pour caractéristique fondamentale la complexité. La science de la complexité se focalise sur les interactions entre éléments et systèmes dans une vision globale.

À partir de ce constat et de ce qui a été dit précédemment, il semble légitime de se demander quelle est aujourd'hui la réelle validité des modèles d'accident et leur applicabilité dans des systèmes socio-techniques possédant un degré de liberté élevé et des interactions irrégulières. Quelle est donc l'efficacité d'un modèle d'accident cherchant à prédire les comportements non linéaires et parfois imprédictibles de systèmes sociaux ? Les systèmes socio-techniques sont caractérisés par de grandes fluctuations et par un haut degré de liberté et de non-linéarité. Il s'avère extrêmement difficile de trouver de la linéarité dans un système socio-technique et les outils mathématiques de modélisation rencontrent d'importantes difficultés à prendre en considération des changements technologiques ainsi que les facteurs humain et organisationnel. Par conséquent, appliquer des outils exclusivement mathématiques au sein de systèmes sociaux serait une erreur. Selon Ilya Prigogine[27], « la complexité est une propriété qui vient du non-équilibre et de la non-linéarité » [Prigogine, 2002]. À la différence de Bertalanffy pour lequel la « théorie générale des systèmes » décrit des systèmes en état d'équilibre stable [Bertalanffy, 1968], Ilya Prigogine a étudié le comportement des systèmes loin de l'équilibre. Les systèmes socio-techniques sont typiquement des systèmes dynamiques loin de l'équilibre et non isolés soumis à des contraintes aussi bien internes qu'externes. Ce sont des systèmes incertains faisant l'objet de processus irréversibles et constituant ainsi des

26 Ce temps est appelé « temps de Lyapounov », noté λ, au-delà duquel le comportement d'un système devient chaotique et toute prédiction devient impossible. Ce temps caractérise un attracteur chaotique lorsqu'il devient positif ($\lambda > 0$).

27 Prix Nobel de chimie en 1977

systèmes de non-équilibre ayant une production d'entropie (de désordre) non nulle inversement proportionnelle à leur degré d'information. Cette entropie peut rester et s'ajouter au système ou bien être « éjectée » du système lui permettant ainsi de s'équilibrer. Il est important de noter que système de non-équilibre n'est pas synonyme de système instable. Un système de non équilibre se distingue d'un système proche de l'équilibre (c'est-à-dire dans le régime linéaire). Dans le cas d'un système de non-équilibre comme un système socio-technique, des fluctuations peuvent se développer et faire migrer le système vers un nouvel ordre. En fait, les processus irréversibles stabilisant les états d'équilibre peuvent jouer un rôle déstabilisateur et provoquer des changements importants d'état [Prigogine, 1979]. Les attracteurs caractérisant ces comportements des systèmes socio-techniques sont dits « étranges » car composés de trois variables au moins, liées par des interactions non linéaires et itératives. Les systèmes socio-techniques présentent également une forte sensibilité aux conditions initiales. En effet, qu'ils représentent une organisation industrielle, un groupe d'individus ou bien une société, ces systèmes peuvent avoir des comportements très divergents dès lors qu'une modification des conditions initiales est apportée. Les comportements de ces systèmes socio-techniques peuvent être qualifiés de chaotiques. Ils sont caractérisés par un manque total de linéarité, ce qui constitue un véritable obstacle à l'application de lois mathématiques et de prédiction. Dans ce cadre, une approche analytique est la plupart du temps inexploitable dans des systèmes socio-techniques constitués d'un nombre important d'éléments interagissant entre eux de façon non linéaire et possédant des rétroactions positives.

Un système dynamique non linéaire soumis à des perturbations peut se mettre à osciller de façon plus ou moins contrôlée en raison de phénomènes de résonance. Ce phénomène de résonance a tout d'abord été expliqué par Poincaré [Poincaré, 1908] afin de montrer qu'il était impossible d'éliminer les interactions entre les éléments d'un système (dans les systèmes dits non intégrables, c'est-à-dire non linéaires). Ce phénomène a été démontré à partir des années cinquante grâce au théorème de Kolmogoroff, Arnold et Moser (dit théorème KAM) [Kolmogoroff, 1954] stipulant, qu'en raison de résonances, peuvent apparaitre deux types de trajectoires : des trajectoires régulières déterministes mais aussi des trajectoires irrégulières et imprévisibles résultant de résonances [Prigogine, 1993]. Poincaré a également démontré que, dans les systèmes dynamiques non intégrables, l'existence de résonances entre les degrés de liberté du système (éléments) en constitue une propriété — cette propriété augmentant, *de facto*, le degré de liberté du système. La notion de résonance a un rapport direct avec celle de fréquences. D'un point de vue physique, la résonance se produit à partir de deux fréquences liées par un rapport numérique simple. Chacun des degrés de liberté (variables) d'un système dynamique est caractérisé par une fréquence. La valeur des fréquences dépend du point de l'espace des phases. Ces résonances de Poincaré jouent un rôle fondamental en physique et peuvent jouer leurs rôles dans les sciences humaines et dans l'analyse des accidents.

La théorie KAM étudie plus particulièrement l'influence de ces résonances sur les trajectoires. Ces résonances mènent à un couplage entre évènements entraînant une rupture de déterminisme et introduisent de l'incertitude tout en brisant la symétrie du temps [Prigogine, 1996]. Ces notions de résonance et de couplage rappellent les travaux de Charles Perrow dans le domaine de la sécurité et sa notion de couplage fort [Perrow, 1984] associé à des interactions complexes (non linéaires) mettant en exergue une part d'incertitude. De façon plus récente, cette notion de résonance amène aux travaux d'Erik Hollnagel et à sa méthode FRAM (*Functional Resonance Analysis Method*).

Dans cette méthode, un système socio-technique est décrit par ses fonctions (approche fonctionnelle) et ses activités plutôt que par sa structure (approche structurelle comme cela est le cas dans le modèle STAMP). FRAM s'attache à représenter la dynamique d'un système en modélisant les interactions non linéaires et leurs performances. Hollnagel s'appuie dans sa méthode sur la notion de résonance stochastique consistant en l'ajout d'un signal (d'un bruit) sur un signal périodique en vue d'obtenir une résonance [Hollnagel, 2004]. Il l'applique pour expliquer l'apparition d'un accident. La méthode FRAM permet d'analyser les systèmes socio-techniques au travers de leurs fonctions et non de leurs structures. FRAM permet en outre d'analyser le comportement d'un système en modélisant ses dépendances non linéaires de ses fonctions ainsi que la variabilité de sa performance. FRAM est fondée sur quatre principes :

- le premier principe stipule que les réussites et les échecs résultent de l'adaptation des organisations face à la complexité (phénomène de désynchronisation) ;
- le deuxième principe souligne que les systèmes socio-techniques ne sont que partiellement prédictibles (phénomène de non-linéarité) ;
- le troisième principe établit que la variabilité de plusieurs fonctions peut mener à des conséquences importantes (phénomène de dépendance sensitive aux conditions initiales) ;
- le quatrième principe précise que la variabilité de plusieurs fonctions peut entrer en résonance, pouvant conduire à l'accident.

D'un point de vue méthodologique (figure 35), FRAM se décompose en 4 étapes :

- une première étape permet d'identifier les fonctions principales du système et de caractériser ces fonctions grâce à 6 critères : entrants (I), sortants (O), préconditions (P), ressources (R), temps (T), et contrôle (C) ;
- une deuxième étape caractérise la variabilité potentielle au travers des conditions communes de performance (CPC) dans un contexte donné. Ces conditions sont au nombre de 11 (disponibilité du personnel et de l'équipement, entraînement et préparation, qualité de la communication, interaction homme-machine, disponibilité des procédures, conditions de travail, but et conflits, temps disponible, rythme circadien ou stress, travail en équipe et qualité organisationnelle). Pour chaque fonction, les facteurs humain et organisationnel sont pris en compte ;

- une troisième étape vise à définir la résonance fonctionnelle fondée sur le couplage possible parmi les fonctions et la potentielle variabilité fonctionnelle ;
- enfin, une quatrième étape sert à identifier les barrières de variabilité.

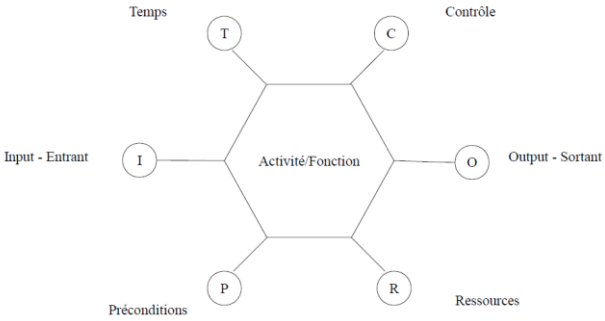


Figure 35 ■ Module FRAM décrivant une activité ou une fonction à partir de six aspects
adapté de Hollnagel, 2004
A noter que cette approche fonctionnelle de la méthode FRAM se focalise sur l'état final du système en plaçant le sujet dans un contexte plus large que le système auquel il appartient.

Lors de l'étape 3 de la méthode FRAM, la résonance fonctionnelle est déterminée à partir du couplage entre fonctions. Ce couplage caractérise la présence de résonances et donc de bruits au sein du système. Cette notion de bruit fait l'objet de la sous-section suivante.

3.2.2. Le concept de « bruit » systémique

Le « bruit » est considéré comme un signal supplémentaire sur le signal d'une variable pouvant avoir une influence plus ou moins importante sur le comportement d'un système. Le chaos dans un système n'est pas dû à un bruit externe [Kiel, Elliot, 1997]. L'analyse du bruit dans un système peut nécessiter une approche analytique du système dans son ensemble [Sterman, 2000] — il s'agit là encore de la complémentarité entre les approches systémique et analytique [De Rosnay, 1995]. Le bruit est une propriété de l'environnement alors que le signal est une propriété du système. Dans une démarche d'analyse de bruit, ce problème peut être réglé par l'application de délais permettant de créer des filtres de variabilité et de séparer un signal d'un bruit. Néanmoins, la performance même d'un système peut être fortement impactée par la présence d'un bruit [McDonnell, Abbott, 2009].

La notion de bruit est inévitablement présente dans les systèmes de non-équilibre [Prigogine, 1977] qui sont par ailleurs des systèmes « excitables ». « L'excitabilité » est un phénomène typiquement dynamique. Un système est dit excitable lorsqu'il possède un point fixe dans un bassin d'attraction. Dans tout système dynamique, existent trois types d'états d'excitabilité : un état de repos, un état excité et un état réfractaire. Pour un système non perturbé et en état d'équilibre stable, l'état de repos

prévaut. De petites perturbations se traduiront uniquement par des réponses linéaires du système [Lindner, Garcia, Neiman, 2003]. C'est un comportement que l'on retrouve dans les systèmes à l'équilibre de Bertalanffy [Prigogine, 2001]. Lorsqu'une perturbation assez forte impacte le système, ce dernier peut sortir de son état de repos, passer par un état excité puis, après un état réfractaire, revenir à un état de repos. La réponse est dans ce cas fortement non linéaire avec une forte variation des variables dans l'espace des phases [Lindner, Garcia, Neiman, 2003]. Cet état excité caractérise l'état d'un système complexe. À noter par ailleurs, qu'en présence de systèmes couplés, les comportements et l'excitabilité engendrés peuvent significativement varier. De tels systèmes de non-équilibre doivent être maintenus par le biais de contraintes et de rétroactions supplémentaires. Une nuance doit être apportée : l'excitabilité est ici présentée dans le cadre de systèmes dynamiques selon la théorie générale des systèmes de Bertalanffy. Dès lors, l'excitabilité d'un système socio-technique variera notamment dans la définition des états de repos selon que le système est dans un état d'équilibre stable ou présente un point fixe. Or, il a été démontré plus haut qu'un système socio-technique ne possède pas de point fixe et ne peut donc au « mieux » se trouver que dans un état d'équilibre instable.

Tous les systèmes socio-techniques contiennent du bruit ou sont sujets à des sources extérieures de bruit. Ce bruit peut être la source de perturbations et de modifications du rythme du système. Chaque système socio-technique est rythmé par des phases et des évènements tout au long de son cycle de vie. Un tel système contient des variables soumises à un bruit créant des oscillations et des variations corrigées par des contrôles et des contraintes. Des oscillations peuvent amener le système à changer de comportement et à adopter un comportement chaotique devenant alors imprédictible. Un système socio-technique peut être « sûr » grâce à un ensemble de contraintes et de contrôles. « La nature stochastique et imprédictible de l'action humaine individuelle est aujourd'hui bien acceptée ; mais très longtemps a perduré la croyance que, pris en masse, le comportement social humain tend à suivre des voies générales et prédictibles. En d'autres termes, s'il existe un bruit notable au niveau du comportement individuel des personnes, il existerait des courants profonds dans les sociétés humaines qui ne sont guères affectés par le bruit et la fureur des évènements quotidiens » [Prigogine, 2001]. Par conséquent, un système « bruité » est un système non linéaire pour lequel peuvent apparaître de grands écarts dans le processus de décision — et notamment entre des conditions apparentes et des conditions désirées [Forrester, 1961]. Ce bruit est très souvent écarté lors de la modélisation d'un système et peut constituer une source importante d'omissions en raison de son caractère incertain.

Les notions de bruit et d'attracteur invitent à s'interroger sur l'acceptabilité des risques par imposition de contraintes afin de maintenir un système au sein de « limites de sécurité », comme le préconise l'approche traditionnelle de maîtrise des risques. Or, la simple création de « limites » va contraindre le système dans son adaptabilité à d'éventuelles perturbations. Plutôt que l'application systématique de

telles contraintes, il semble préférable de favoriser la synchronisation entre le système et son environnement afin de maintenir une adéquation entre leurs évolutions respectives, évitant que le système ne bascule, à un moment ou à un autre, vers un changement d'état. Ce besoin de synchronisation reflète le caractère « rythmique » des systèmes dynamiques non linéaires, les faisant passer d'un comportement à un autre par le biais de « bifurcations ». De tels rythmes ont pour fonction de permettre l'adaptation aux variations prévisibles du milieu environnant, voire leur anticipation [Prigogine, 2001]. « Lorsque ce milieu connaît des variations imprédictibles, les rythmes réagissent à ces changements et procurent une versatilité accrue. Un rythme possède en effet un degré de liberté de plus qu'une réponse non oscillante dont seule l'amplitude varie, alors que pour les rythmes l'amplitude et la période peuvent toutes deux changer en réponse à une variation de l'environnement » [Prigogine, 2001]. C'est pourquoi l'imposition de contraintes au sein d'un système ne doit pas empêcher ce dernier d'intégrer, grâce à ses rythmes, des variations imprévues du milieu environnant, afin de lui permettre de se positionner sans dommage sur une trajectoire « sûre » pour éviter un bassin d'attraction accidentel et lui autorisant ainsi une synchronisation continue avec son environnement. Cette synchronisation caractérise la capacité d'un système à s'auto-organiser[28] et à développer de nouvelles structures de contrôle pour se maintenir dans un état « sûr » et d'éviter des comportements chaotiques.

3.2.3. Vers un premier modèle d'accident « chaotique »

L'analyse des systèmes socio-techniques s'attache à prendre en considération leurs propriétés systémiques et montre comment un système peut s'auto-organiser pour maintenir une stabilité structurelle lorsqu'il se trouve loin de l'équilibre sans qu'une force extérieure agisse sur lui. Ce comportement complexe est non linéaire et les liens entre causes et effets ne peuvent être identifiés [Bertuglia, Vaio, 2005]. Les rétroactions positives des systèmes complexes sont génératrices d'évolution et font émerger la « flèche du temps » ; ils doivent par conséquent être inclus dans le processus de contrôle. Les cycles de rétroactions positives amplifient les effets des perturbations (phénomène d'autocatalyse) augmentant l'amplitude des fluctuations. Ce sont ces rétroactions positives qui mettent le système loin de l'équilibre et qui permettent de caractériser des résonances et de le faire évoluer.

Ilya Prigogine doit l'attribution du prix Nobel de chimie en 1977 à ses travaux sur les systèmes dissipatifs et sur la notion de « flèche du temps » [Prigogine, 1988]. Un

28 « Le terme auto-organisation fait donc référence à un processus dans lequel l'organisation interne d'un système, habituellement un système en non équilibre, augmente automatiquement sans être dirigée par une source extérieure. Typiquement, les systèmes auto-organisés ont des propriétés émergentes. L'auto-organisation désigne l'émergence spontanée et dynamique d'une structure spatiale, d'un rythme ou d'une structure spatiotemporelle sous l'effet conjoint d'un apport extérieur d'énergie et des interactions à l'œuvre entre les éléments considérés » [Paris, 2009].

système dissipatif importe de l'énergie et/ou de l'information provenant de l'environnement qu'il dissipe en son sein, provoquant des réajustements caractérisés par l'émergence de la « flèche du temps » et par la formation de nouvelles structures n'existant pas à l'état d'équilibre stable. Contrairement à un système dissipatif, un système à l'état d'équilibre stable ne se réorganise pas, mais libère uniquement de l'énergie sans l'absorber et tend vers un attracteur dit « point limite ». L'exemple le plus représentatif est la bille qui, placée au fond d'une cuvette, atteint une position fixe après avoir libéré son énergie.

Les structures dissipatives émerge donc d'un processus d'auto-organisation [Paris, Sperber, 2009] se traduisant par un réajustement des paramètres de contrôle du système et par l'émergence de la « flèche du temps » caractéristique de processus irréversibles et d'évolution.

Le phénomène d'auto-organisation modifie la structure du système sans l'intervention d'une force extérieure le poussant sur une trajectoire d'un nouvel attracteur représentant un nouvel état organisé. Concrètement, les fluctuations font faire migrer le système d'un bassin d'attraction vers un autre bassin d'attraction. Ce passage entre un bassin à un autre est spontané et n'est dû qu'aux fluctuations dans des conditions de déséquilibre sans intervention extérieure. L'auto-organisation doit être distinguée du phénomène de *sélection*, qui désigne l'accomplissement d'un choix entre différents états de stabilité et donc d'états en compétition, dû à la pression d'une force extérieure sur le système. L'auto-organisation est un nouvel ordre émergent, un ordre du non-équilibre [Bertuglia, Vaio, 2005]. Le système peut alors afficher des propriétés émergentes et des nouvelles structures émergentes sensibles aux valeurs des paramètres de contrôle.

Cette nouvelle structure dissipative émergeant par auto-organisation est une structure instable pouvant être facilement dissoute en raison d'une modification dans les valeurs des paramètres de contrôles. Il y a une inadéquation entre la nouvelle structure et les paramètres de contrôle. Une structure dissipative reste donc fragile, contrairement à une structure en état d'équilibre.

Face à ces constats, les modèles d'accident systémiques montrent leurs limites dans leur démarche d'étude et d'analyse d'un système loin de l'équilibre. Un système socio-technique n'est jamais à l'état d'équilibre stable et se trouve même loin de l'équilibre. Par conséquent, un tel système est un système dissipatif [Prigogine, 1984] voire adaptatif doté d'une capacité d'auto-organisation et d'autoreproduction lui permettant de modifier sa structure et de se maintenir à l'équilibre par dissipation (gestion) de flux (matière, énergie, information).

Il est alors légitime de se demander si l'accident n'est pas le résultat d'un phénomène spontané d'auto-organisation se traduisant comme le « passage »[29] ou

29 Ces notions de passage, de catastrophe et d'influence de bassin appartiennent également au corpus théorique développé par René Thom sous le nom de « théorie des catastrophes » [Thom, 1991].

une « bifurcation » d'un bassin d'attraction à un autre, résultant d'un phénomène d'autocatalyse (rétroaction positive). Le choix de qualifier l'accident d'« incident » ou de « catastrophe » dépendrait du couplage entre deux bassins d'attraction, c'est-à-dire de la *différenciation* et de la *connexion* entre deux bassins d'attraction (figure 36). Un couplage fort (une forte connexion) provoquerait un phénomène d'« incident », réversible, lors d'un changement de bassin tout simplement parce qu'un couplage fort permet un passage plus « doux » entre deux bassins.

Supposons qu'un système A (se trouvant dans un bassin A) et un système B (se trouvant dans un bassin B) sont deux systèmes différents dont le passage (la bifurcation, l'accident) de A vers B se fait de façon imprédictible et possédant de nombreux éléments en commun. Plus le couplage (connexion) est fort entre ces deux systèmes de bassins différents, plus le nombre d'éléments en commun est grand et moins le passage (la bifurcation, l'accident) du bassin A vers le bassin B provoque de changements (de dommages) en raison d'une faible différentiation.

À l'inverse, plus la connexion est faible entre deux systèmes de deux bassins différents, plus le nombre d'éléments en commun est faible et plus la bifurcation du bassin A vers le bassin B provoque de changements (de dommages) en raison d'une forte différentiation. Une faible connexion provoquerait un phénomène catastrophique, irréversible, en raison du passage forcé vers un bassin n'ayant que peu de « correspondances » avec le bassin d'origine.

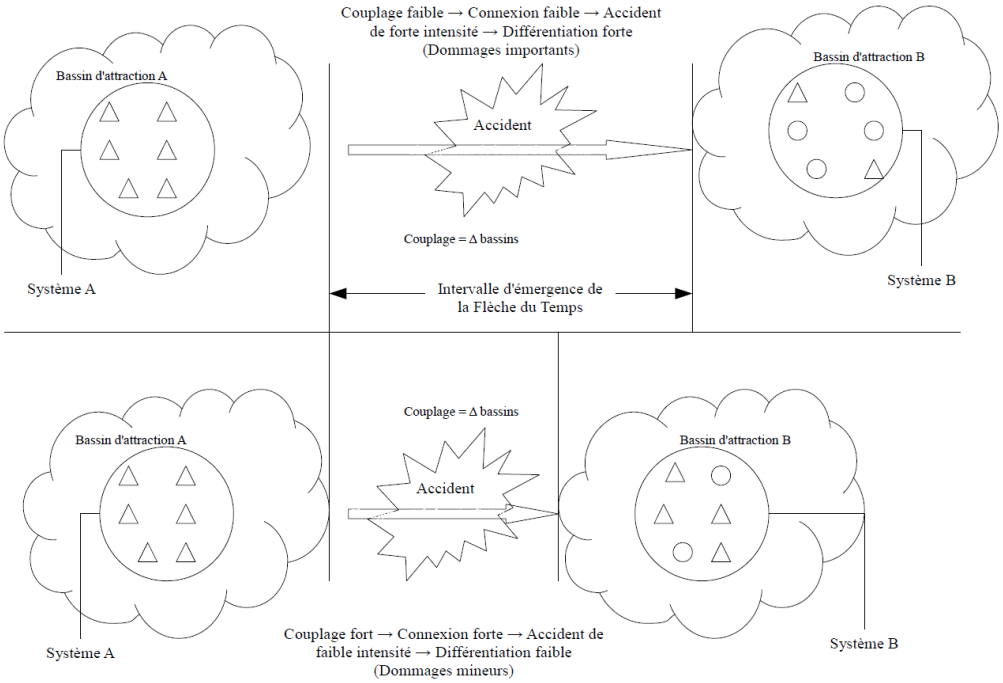


Figure 36 ■ Caractérisation de l'accident selon la nature du couplage entre deux bassins d'attraction

Il est alors possible de proposer un cycle d'évolution d'un système dynamique (figure 37), tel qu'un système socio-technique, prenant en considération des

perturbations et lui permettant de se maintenir dans un état d'équilibre malgré des fluctuations, voire des changements d'attracteurs, par le biais de bifurcations.

Ce cycle se fonde sur plusieurs théories : la théorie des systèmes et du contrôle, la théorie du chaos, la théorie de la complexité et la théorie des structures dissipatives ; il permet de poser les fondements d'un modèle d'accident chaotique.

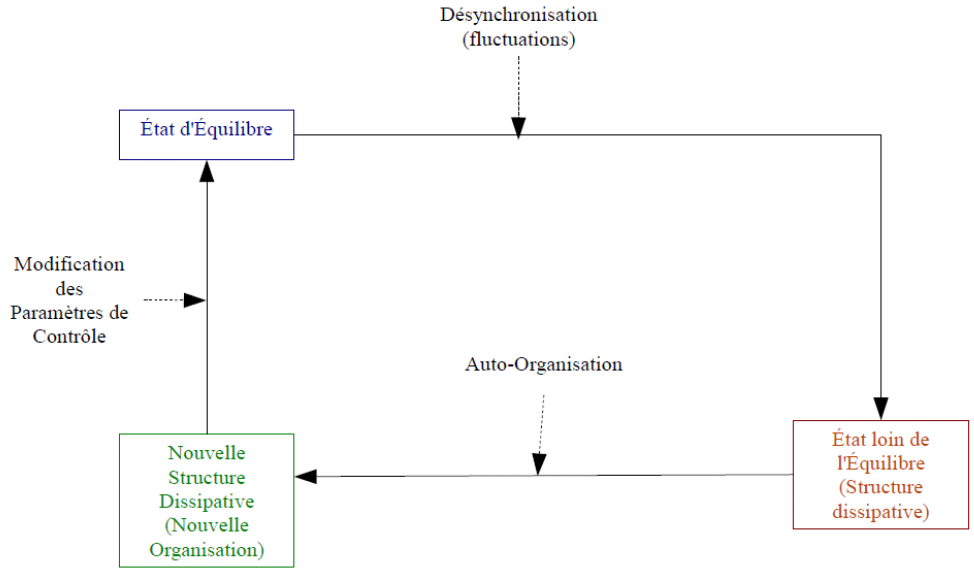


Figure 37 ■ Cycle de réponse d'un système désynchronisé

Par le jeu des fluctuations, un système peut se trouver dans un état d'équilibre stable, complexe ou chaotique. Cette évolution dépend du niveau de contrôle et de synchronisation. C'est dans un état de complexité qu'un système peut créer de nouvelles configurations et engendrer des propriétés émergente (comme la sécurité)[30]. La complexité se traduit par un changement d'état consécutif à une instabilité interne et/ou une action externe sur le système. La dynamique d'un système complexe est donc caractérisée par des trajectoires sensibles aux perturbations d'origine interne et externe [Bertuglia, Vaio, 2005]. L'objectif fondamental d'un tel cycle est d'éviter une désynchronisation « chronique » entre le système et l'environnement, poussant le système à sa limite de prédiction (correspondant à un « temps de Lyapounov » positif et synonyme de prédictions impossibles et de fortes incertitudes [Prigogine, 2001]) et pouvant le faire passer, en l'absence de contrôles adéquats, vers un nouveau bassin d'attraction par le biais d'un accident (*v.* figure 36).

Par conséquent, les systèmes socio-techniques sont par essence des systèmes complexes, en état d'équilibre instable, pouvant cependant présenter un niveau élevé

[30] Alors que les modèles d'accident traditionnels sont à l'origine d'une confusion entre stabilité et sécurité

de sécurité. Le fait qu'un système soit en équilibre instable n'est en effet pas synonyme d'insécurité.

Un système purement technique, peut, quant à lui, être dans un état d'équilibre stable, complexe ou même chaotique.

3.2.4. Le phénomène « accident » dans un système socio-technique

La notion « d'état accidentel » dans un système[31] a été présentée dans le chapitre 2. Cette définition requiert quelques amendements dans le cas d'un système socio-technique puisque les relations n'y sont plus linéaires.

L'accident — si l'on se réfère à la définition que propose la théorie des systèmes dynamiques non intégrables et présentée dans l'introduction de ce chapitre — est un évènement irréversible et imprédictible dû une absence de réponse adaptée, faisant suite à une réorganisation non contrôlée dans un contexte donné et pouvant mener à des dommages et des pertes. Autrement dit, l'accident est donc un phénomène de collision, de brisure de symétrie, de bifurcation ou de transition d'un système à un autre, engendré par une absence de réponse adaptée d'un système suivant une réorganisation non contrôlée de sa structure dans un contexte donné.

L'analogie est, sur certains points cruciaux comme les notions de transition, de structure et de contexte, manifeste entre ces deux définitions ; elle ne doit toutefois pas masquer certaines disparités.

La première est que l'état accidentel d'un système dynamique intégrable est une fin en soi, une étape, un évènement en bout de chaîne, un état d'un système au cours du temps. Cet état se caractérise dans l'esprit des individus par le résultat de la réalisation d'un risque — par exemple, un attentat terroriste (le risque) peut provoquer de nombreuses victimes et/ou dommages matériels. Cet état de dégradation caractérise l'« image » que l'on peut avoir d'une situation résultant de la réalisation d'un risque. Dans le cadre d'une vision « chaotique » de l'accident, ce dernier n'est plus une fin en soi ou un état du système à un instant t donné, mais une « brisure de symétrie » générant sa propre flèche du temps. L'état accidentel chaotique dans un système socio-technique ne peut être lu comme un état d'un système à un instant t puisque cet état n'existe que par l'existence d'un temps (sa flèche du temps).

L'accident chaotique se traduit comme un phénomène irréversible (un changement générant sa flèche du temps) et imprédictible (caractérisant le comportement chaotique d'un système socio-technique à un « instant t de sa flèche du temps ») dû à une perte de contrôle du système dans un contexte donné. Le

31 Un état accidentel est considéré comme le résultat d'un phénomène accidentel se traduisant par une nouvelle configuration systémique caractérisée par une transition de phase au niveau de ses processus, de sa structure et/ou de sa fonction dans un contexte donné se traduisant par une dégradation du système.

« phénomène accidentel » est spontané et ne se réalise que lors d'un comportement chaotique d'une structure dissipative d'un système socio-technique (dépendant directement de sa structure) le poussant vers un « nouveau » système dissymétrique.

Ce « passage » d'un système S_1 à un système S_2 traduit l'accident pour lequel les dommages (D) et les pertes sont la différence $D(S_1 - S_2)$. *A priori*, pour des dommages et des pertes, cette différence reste toujours positive jusqu'au rétablissement d'un état d'équilibre du système S_2 et peut devenir négative dans le cadre d'une démarche de retour d'expérience ou d'une démarche d'apprentissage organisationnel. En effet, l'objectif d'un retour d'expérience est une réorganisation structurelle afin de faire émerger, au travers de contrôles adéquats, une synchronisation d'un système socio-technique avec son environnement. L'état d'équilibre résulte de contrôles adéquats dans un contexte donné (figure 38). Ce temps de rétablissement ou d'application de contrôles adéquats correspond à la notion de « crise » durant laquelle une structure dissipative (encore fragilisée) prend en considération un contexte et dissipe de nouvelles informations adéquates au niveau de sa structure pour définir des contrôles adéquats qui stabiliseront la structure par évacuation d'entropie. Le temps de « crise » est le temps nécessaire à la structure pour dissiper un flux (d'information, de matière, d'énergie) nouveau menant à l'équilibre. Durant une « crise », tant que le système ne retrouve pas un état d'équilibre, d'autres accidents peuvent survenir.

L'accident doit être distingué d'un simple changement organisationnel par le caractère « imprédictible » inhérent à sa nature. Un changement organisationnel dans un système socio-technique peut être quant à lui irréversible mais reste prédictible.

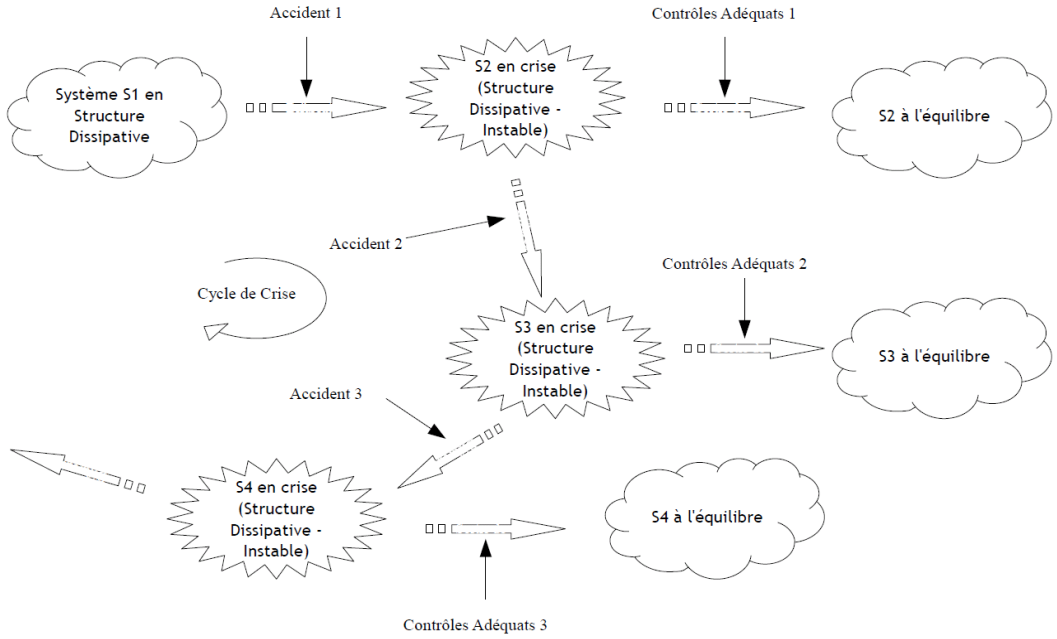


Figure 38 ■ Cycle de crise et de rétablissement d'un système socio-technique

Exemple : La plateforme pétrolière Deepwater Horizon

L'explosion de la plateforme *Deepwater Horizon* de BP en avril 2010 a entraîné la mort de onze personnes et le naufrage de la plateforme.

Avant explosion, cette plateforme est un système socio-technique, donc complexe (S_1 dans la figure 38) d'exploitation de gisements pétroliers en haute mer, composé d'un nombre important d'interactions non linéaires et présentant un état d'équilibre instable. Cet état ne dépend pas directement d'éventuelles pressions externes et est donc un état d'équilibre instable par nature (car complexe). L'enjeu sécuritaire pour la plateforme est alors de maintenir une stabilité structurelle synonyme de sécurité au regard de contraintes économiques/productives (son environnement).

Les pressions grandissantes (ici, les changements environnementaux) perturbent le système « Deepwater Horizon » ou système BP et sont à l'origine de sa désynchronisation « chronique » avec son environnement. Cette désynchronisation provoque la formation d'une structure dissipative (structure instable) issue d'un phénomène d'auto-organisation. Le phénomène d'auto-organisation se retrouve dans tout système socio-technique permettant au système de se restructurer sans action extérieure. Cependant, le système BP n'a pu être reconfiguré (mise à jour des paramètres de contrôle) à temps pour répondre de façon adéquate à ce changement La plateforme est un système socio-technique générant sa propre flèche du temps et donc ses changements irréversibles. Ces derniers peuvent être plus ou moins bien intégrés au sein de la structure dissipative, impliquant un effort permanent d'adaptation et de contrôle.

Au sein du système BP, la mise à niveau des paramètres de contrôle (notamment la vérification et le contrôle de la valve de sécurité installée à l'entrée du puits servant à gérer les problèmes de pression) s'est avérée trop longue et le « temps de Lyapounov » considéré comme le passage vers un comportement chaotique (et donc imprédictible) a été atteint ($\lambda > 0$).

Ce comportement chaotique s'est traduit par un flux incontrôlé d'hydrocarbure remontant dans le puit, libérant des gaz à l'origine de l'explosion (accident 1). Cet accident a mené à un système dissipatif (S_2) extrêmement endommagé (S_1 et S_2 devaient être faiblement couplés). Ce « nouveau » système S_2, est un système socio-technique fortement instable en « crise ». Le but des sauveteurs est alors de stabiliser ce système pour le sortir de son cycle de crise. Cependant, le système S_2, correspondant à la plateforme « Deepwater Horizon » en feu n'a pu être stabilisé à temps par le biais de contrôles adéquats. On assiste alors à une seconde bifurcation (S_2 vers S_3) menant au naufrage (à la destruction complète) de la plateforme (S_3 à l'état d'équilibre stable – la plateforme est réduite à cet instant (on peut ici parler d'instant) à un simple système technique dont le comportement peut être étudié au travers de la théorie général des systèmes de Bertalanffy).

Le système n'a pas pu atteindre un nouvel attracteur du même bassin d'attraction (bassin A) et est devenu incontrôlable (comportement chaotique) ; son comportement devient alors imprédictible (son attracteur est un attracteur chaotique).

Le système BP a subit de fortes pertes après la première explosion (accident 1) résultant d'une bifurcation (un passage spontané irréversible en raison des non-linéarités) du bassin A au bassin B. La trajectoire du système se trouve alors dans le bassin d'attraction B.

Nous sommes en présence d'un système B, ayant subi de forts dommages et constituant à ce jour un système purement technique dans un état d'équilibre stable, le comportement est devenu linéaire et prédictible (le système est détruit, donc « mort ») et évolue donc au cours du temps, ne présentant plus de flèche du temps. Le système ne subit alors qu'une dégradation par libération d'énergie (auto-inhibition).

Les forts dommages (forte différenciation) amènent à penser que le système A (avant explosion) et le système B (système actuel) étaient fortement connectés et donc faiblement couplés. Ce couplage (rapprochement) entre deux systèmes de bassins différents résulte d'un phénomène d'autocatalyse non contrôlée. Le bassin B est venu « arracher » de façon violente le système A pour le faire bifurquer vers le bassin B.

L'accident peut donc être décrit comme un évènement ou un phénomène irréversible et imprédictible, voire comme un changement irréversible et imprédictible d'un système socio-technique au regard de son environnement, dû à un manque de réponse adaptée au niveau de sa structure. Il se traduit par une bifurcation d'un espace de phase « sûr » vers un nouvel espace de phase (« sûr » ou « non sûr »), induisant une brisure de symétrie. À l'équilibre instable, le système est

symétrique. Or, le phénomène accident fait spontanément émerger au cours de sa flèche du temps une bifurcation, qui ne doit pas être vue comme menant irrémédiablement à des pertes ou à des dommages mais comme devant imposer une réponse du système afin d'éviter toute perte ou simplement d'évoluer voire de se perfectionner.

L'accident, en théorie du chaos, ne devrait pas être systématiquement perçu en termes de pertes ou de dommages mais comme le « besoin » pour un système de s'équilibrer et de se retrouver « en phase » avec son environnement, lui permettant, au travers de processus d'auto-organisation, de se maintenir dans un état d'équilibre. Il peut sembler original, voire périlleux, de voir l'accident comme un « besoin » mais il est aussi capital de rappeler que ce besoin reste indépendant de toute volonté sociale et qu'il est toujours irréversible et imprédictible.

Cette définition de l'accident permet de le différencier d'un évènement irréversible et prédictible comme un acte terroriste, une crise ou un simple phénomène « incident » (figure 39).

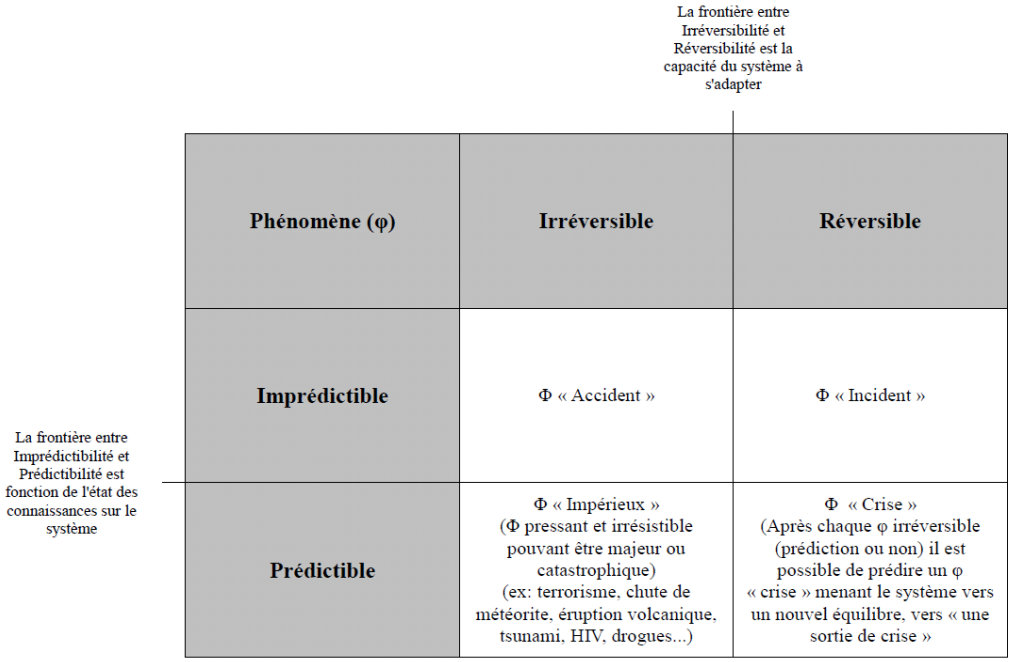


Figure 39 ■ Qualification d'un phénomène (Φ) en fonction de ses caractères réversible et prédictible

Le double caractère d'irréversibilité et d'imprédictibilité permet donc de définir ce qu'est un phénomène « accident ». Un phénomène prédictible et irréversible dont les conséquences mènent à un phénomène pressant et irrésistible est dit « impérieux ». Un phénomène impérieux empêche tout système d'atteindre son objectif ; le système y est hors de contrôle, se traduisant par des dommages et des pertes sur sa structure,

l'empêchant de remplir sa fonction dans un contexte donné[32]. Ce type de phénomène peut mener soit à un phénomène qualifié de « crise », soit à d'autres phénomènes « accidents ». Cette dynamique est due au comportement non linéaire et imprédictible d'un système socio-technique.

Un phénomène imprévisible mais dont les conséquences sont réversibles et ne mènent pas à une perte de contrôle est quant à lui qualifié de phénomène « incident ». C'est donc la capacité d'un système à produire une réponse adaptée dans un contexte donné qui délimite la frontière entre la réversibilité et l'irréversibilité d'un phénomène.

La série de phénomènes « accident », « impérieux » et « crise » décrit un espace ou une zone de perte de contrôle (espace des phases incontrôlables au sens de la théorie du chaos) ne permettant pas de maintenir le système en sécurité et pouvant l'empêcher de remplir son objectif (figure 40). Le phénomène « incident » se trouve dans un espace ou une zone de préservation du contrôle (espace des phases contrôlables au sens de la théorie du chaos) permettant un maintien du système sous contrôle afin de remplir un objectif. Il est alors possible de définir une zone de contrôle comme une section de l'espace des phases dans laquelle le système est en « sécurité ».

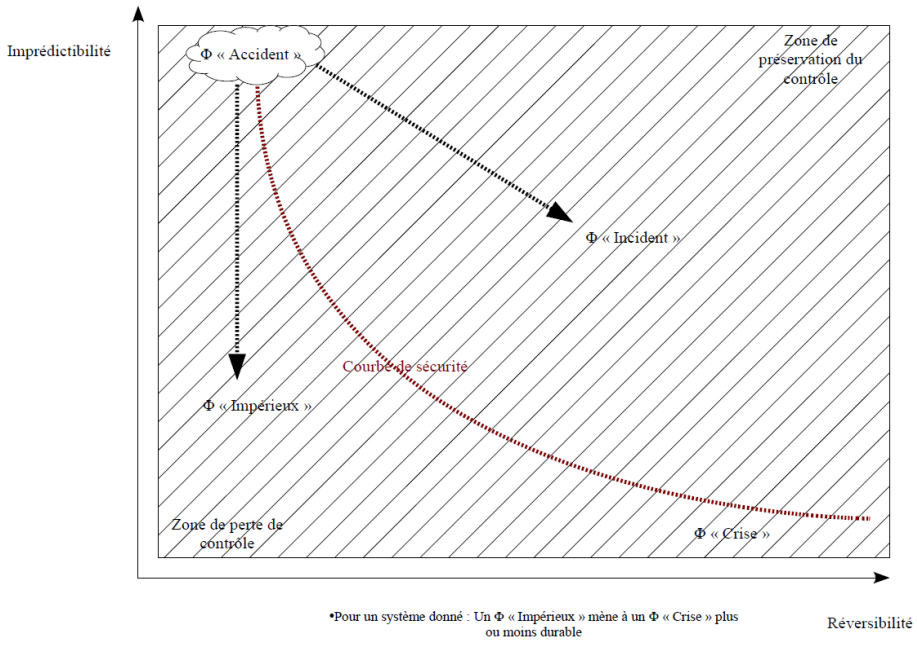


Figure 40 ■ Espace de sécurité d'un système en fonction des phénomènes existants

Le phénomène accident est une bifurcation menant un système à la confrontation avec une réalité imposant une réponse adaptée afin de le maintenir sous contrôle.

[32] Ce contexte est dépendant du niveau d'information et de connaissance disponible. Ainsi, le phénomène « impérieux » caractérisé par une forte entropie deviendra un phénomène « incident » dès lors que le niveau de connaissance sera suffisamment acceptable.

Toute réponse inadéquate mène à un phénomène impérieux. Un système socio-technique est alors qualifié d'adaptatif lorsqu'il est capable d'intégrer au niveau de sa structure dissipative, un nouveau flux (d'information, d'énergie ou de matière) lui permettant de fournir une réponse adéquate lors d'un phénomène accident ne menant qu'à l'incident (figure 41).

Exemple : L'accident du vol US Airways 1549

Le 15 janvier 2009, un Airbus A320 de la compagnie aérienne US Airways se pose d'urgence sur le fleuve Hudson à New York. Le bilan de cet accident est de 78 blessés sur les 155 passagers et membres d'équipage. La cause de cet accident est la collision avec un vol d'oiseaux ayant provoqué des dommages sur les réacteurs de l'avion, puis une perte de puissance des moteurs. Suite à l'amerrissage forcé sur l'Hudson, plusieurs navettes et bateaux se trouvant à proximité se sont rendus rapidement sur place pour porter secours aux passagers.

Lors de cet évènement, un phénomène accident a provoqué une brisure de symétrie. Cette dissymétrie est due à la présence d'un vol d'oiseaux dans le système (confrontation avec une réalité). Le phénomène imprédictible (collision avec un vol d'oiseaux) mène au phénomène impérieux (l'amerrissage d'urgence sur le fleuve Hudson), source de pertes et de dommages, dû à l'absence de réponse adaptée du pilote face à cet évènement imprédictible. Si ce phénomène imprédictible n'avait pas empêché l'avion de continuer son vol jusqu'à sa destination alors ce phénomène aurait été qualifié de phénomène « incident ». Cette différence de qualification dépend de la capacité d'adaptation du système à faire face à un phénomène imprévisible en apportant une réponse adaptée après avoir intégré un nouveaux flux.

Le phénomène caractérisé par l'assistance des navettes et des bateaux se trouvant à proximité au moment de l'accident est qualifié de phénomène de « crise ». Ce phénomène peut mener à d'autres phénomènes accidents et/ou impérieux mais présente une tendance à atteindre la courbe de sécurité et, par conséquent, à atteindre une sortie de crise.

Au travers de cette qualification de différents phénomènes, il est intéressant de noter que l'accident caractérise une bifurcation d'un espace des phases « sûr » à un autre en raison d'un comportement chaotique. Le phénomène « accident » n'est jamais directement la source de dommages et de pertes alors que le phénomène « impérieux » oui. L'accident considère le changement d'espace des phases mettant en exergue le besoin pour le système de retrouver un état d'équilibre dans un environnement donné et parfois turbulent en intégrant au sein de la structure dissipative le flux nouveau lui permettant de répondre efficacement tout en évacuant son entropie.

Un système voulant faire face au phénomène « impérieux » se doit d'être capable de franchir la frontière entre l'irréversibilité et la réversibilité faisant de lui un système complexe adaptatif ou non.

Dans cette perspective, le phénomène « accident » n'est jamais qualifié de « majeur » ou de « catastrophique » car l'accident ne qualifie jamais un niveau de dommages ou de pertes mais uniquement une brisure de symétrie. Dans ce cadre c'est le phénomène « impérieux » qui peut être qualifié de majeur ou de catastrophique.

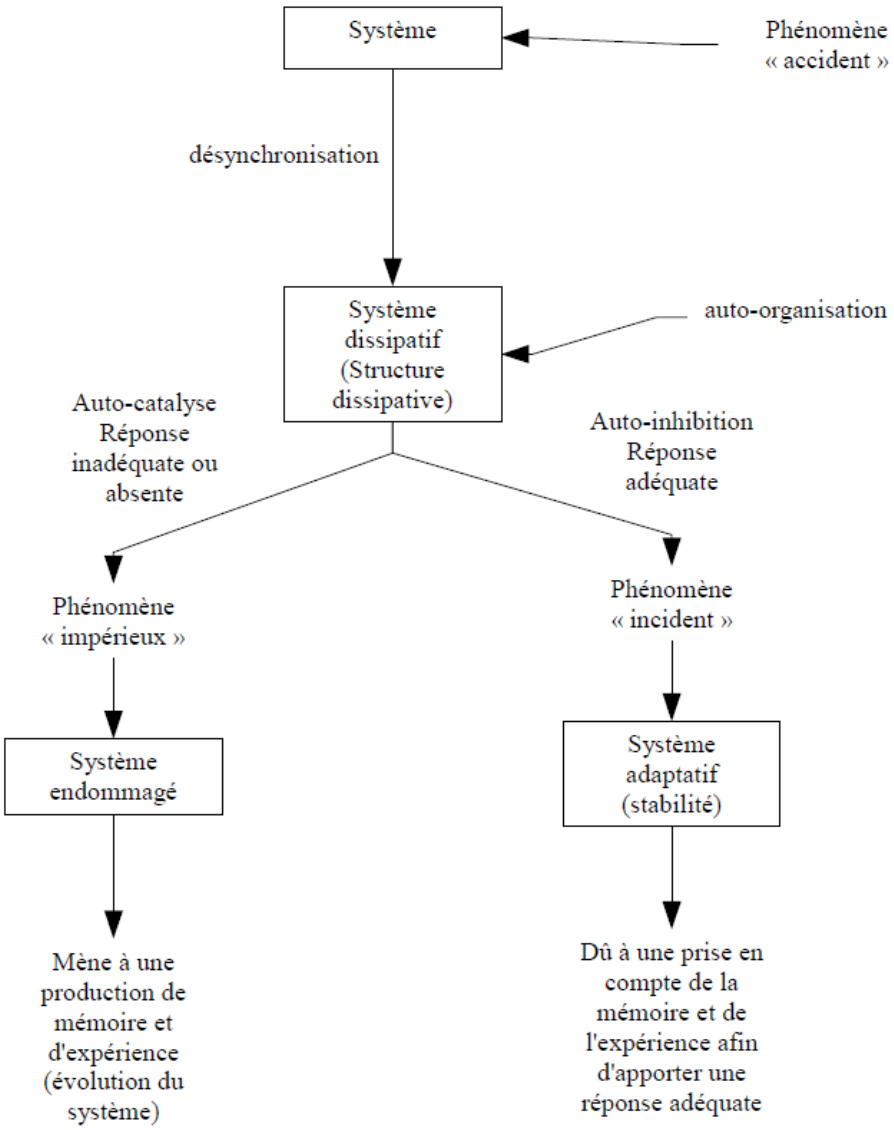


Figure 41 ■ Processus de réponse d'un système face au phénomène accident dans un contexte donné.

Le système dont la structure est dissipative tente de se maintenir dans un espace des phases (ou une section) « sûr » par libération d'entropie en se réorganisant.
Lorsqu'un seuil critique est atteint alors une bifurcation a lieu menant au phénomène impérieux ou incident caractérisant la réponse (inadéquate ou adéquate) du système dépendant de sa mémoire propre.

Conclusion

Ce chapitre a été divisé en trois sections.

Dans un premier temps, il s'est attaché à classer la technique s'analyse des dangers STPA, fondée sur le modèle d'accident STAMP, comme une nouvelle technique en sécurité des systèmes.

Ce chapitre a présenté dans un deuxième temps, une première évaluation du modèle d'accident STAMP en tant que modèle d'accident systémique. Cette deuxième section a permis de cerner les apports et les limites d'un modèle d'accident systémique et son application dans des systèmes tels que les systèmes socio-techniques. Elle permet de montrer que ses apports sont aussi ses limites.

Enfin, la dernière section de ce chapitre présente, au regard des limites des modèles d'accident systémiques, centrée sur les notions d'équilibre et de temps, les perspectives de ce travail de recherches et le besoin d'intégrer de nouveaux concepts issus directement des travaux dans le domaine de la théorie du chaos, de la théorie de la complexité et de la théorie des structures dissipatives permettant de définir les fondamentaux pour un nouveau modèle d'accident.

Cette section a posé le phénomène « accident » comme la bifurcation d'un espace des phases « sûr » vers un autre espace tout en soulignant que ce passage n'est pas systématiquement synonyme de pertes comme dans le cadre de l'approche « classique » de l'accident mais pouvant être source d'évolution voire de perfectionnement.

Conclusions

Ce travail poursuivait cinq objectifs.

■ Un premier objectif a été, au cours du chapitre 1, de présenter la notion d'accident au travers de définitions contemporaines permettant de poser un premier cadre afin de mieux comprendre l'accident au sens commun du terme. L'accident reste, dans la conscience collective, un évènement dangereux qui provoque dommages et pertes.

Ce travail a été essentiel avant de pouvoir introduire et décrire les premiers modèles d'accident apparu au cours du XX^{e} siècle comprenant le modèle « séquentiel » d'Heinrich [Heinrich, 1931] ou les modèles organisationnels de l'accident de Reason [Reason, 1997] ou des HRO et de Perrow [Sagan, 1993]. Ces premiers modèles, dits traditionnels, sont largement implantés dans les modèles cognitifs populaires et industriels et gardent, malgré leurs limites, une place majeure dans les évaluations des risques industriels ou lors d'enquêtes accident. Cette place s'explique en grande partie par le fait que ces modèles se sont développés dans un cadre scientifique occidental, fondé sur des théories scientifiques prédominant depuis les travaux de Newton. Ce cadre pousse à la simplification et à la réduction du système étudié afin de tirer des lois générales de comportements particuliers. Ces modèles traditionnels voient l'accident comme une chaîne d'évènements dont l'accident constitue le dernier maillon, considéré comme un évènement qui survient à un instant donné.

■ Un deuxième objectif a été, au cours du chapitre 2, de présenter et de décrire des modèles plus récents appelés modèles « d'accident systémiques ». Comme leur nom l'indique, ces modèles sont fondés sur la théorie générale des systèmes de Bertalanffy [Bertalanffy, 1968] et sont d'un apport incontestable dans la compréhension des accidents. Ils permettent d'appréhender le système de façon globale, c'est-à-dire en prenant en compte l'ensemble des facteurs ayant pu jouer un rôle dans la migration d'un système vers un état accidentel. Le principal apport des modèles d'accident systémiques par rapport aux modèles d'accident dits traditionnels est la prise en

compte de l'aspect dynamique. Le système évolue au cours du temps et son comportement présente des variations et des organisations différentes au sein de sa structure. Le système est sur une trajectoire et les différents comportements le font migrer ou non vers des limites de sécurité au delà desquelles il atteint un état accidentel.

Ces modèles d'accident systémiques présentent quatre paramètres spécifiques :

- la fonction, caractérisant le but du système ;
- la structure, caractérisant le comportement du système ;
- les processus, caractérisant les interactions entre les éléments du système ;
- enfin, le contexte, caractérisant le cadre d'évolution du système à un moment donné.

C'est à partir de ces quatre caractéristiques de l'accident que les modèles d'accident systémiques permettent de définir la notion d'« état accidentel ». Cette notion caractérise l'état d'un système ayant migré vers l'accident et dont la structure ne lui permet plus de fonctionner dans des conditions de sécurité adéquates.

■ Le troisième objectif a été, au cours du chapitre 3, de présenter un modèle accident systémique appelé STAMP (*System-Theoretic Accident Modeling and Processes*), développé par le Professeur Nancy Leveson du Massachusetts Institute of Technology au début des années 2000. STAMP propose un changement de paradigme dans la manière de concevoir les causes d'un accident.

Alors que les modèles d'accident traditionnels voient l'accident comme résultant d'une chaîne d'évènements, le modèle STAMP postule que l'accident résulte d'un problème de contrôle au sein de la structure d'un système. Ce modèle se fonde à la fois sur la théorie générale des systèmes et sur la théorie du contrôle. Il repose également sur les travaux de Rasmussen [Rasmussen, 1997] prenant en compte les aspects hiérarchique et dynamique d'un système. Il est construit autour de trois concepts : la contrainte, la structure hiérarchique et les modèles de processus (boucles de contrôle). Ce troisième objectif, dépassant la simple introduction du modèle STAMP, a été de décrire une technique d'analyse des dangers appelée STPA (*STAMP-Based Analy*sis), fondée sur le modèle STAMP. Ce travail a permis de décrire la technique STPA pour l'enquête accident et l'évaluation de la sécurité ; travail qui n'avait pas été effectué à ce jour. Cette méthode ne vise pas à être considérée comme la méthode de référence d'application de la technique STPA mais uniquement comme une version préservant l'esprit du modèle d'accident STAMP tel que défini par Nancy Leveson.

■ Le quatrième objectif a été, au cours du chapitre 4, d'expérimenter et d'appliquer la méthode de la technique d'analyse des dangers STPA au sein d'un système industriel. Le cœur du système considéré est un procédé physico-chimique de traitement de sédiments contaminés appelé Novosol® et développé par la société Solvay.

Ce chapitre 4 a été organisé autour d'une triple articulation. Un premier axe présentait la problématique industrielle au sein de laquelle intervient le procédé Novosol® : les sédiments contaminés et leur gestion. Un deuxième volet décrivait le système Novosol® d'un point de vue technique et se polarisait sur le procédé physico-chimique puis d'un point de vue global focalisée sur l'ensemble des interactions entre intervenants. Un troisième angle d'étude traitait de l'intégration de la méthode STPA dans le système Novosol® dans le cadre d'une évaluation de la sécurité.

L'application de la méthode STPA met en exergue les notions de contrainte, de structure hiérarchique et de modèles de processus (boucles de contrôle). L'objectif de cette application a été, au delà de la formulation de recommandations centrées sur le procédé Novosol®, d'établir une stratégie globale d'évaluation de la sécurité permettant une optimisation de la sécurité tout au long du cycle de vie du système Novosol®.

■ Le dernier objectif de ce travail de thèse a été, au cours du chapitre 5, d'apporter un regard critique sur le modèle d'accident STAMP ainsi que sur la technique d'analyse des dangers STPA. Ce chapitre a été construit autour de trois articulations.

La première voyait la technique STPA comme une nouvelle technique de sécurité des systèmes [DoD, 2000], selon des critères empiriques en raison d'un manque certain de critères officiels.

La deuxième articulation s'est intéressée aux apports et aux limites du modèle d'accident STAMP au regard des limites des modèles d'accident traditionnels. Les principaux apports sont centrés sur les notions d'équilibre et de temps. Cette notion d'équilibre concerne directement le cadre scientifique au sein duquel s'inscrit les modèles d'accident systémiques étudiant les systèmes dans des états d'équilibre stables pouvant éventuellement migrer vers des états d'instabilité voire accidentel. La notion de temps est quant à elle également problématique suivant les différents états d'un système. Cet axe de réflexion a permis de souligner que les apports des modèles d'accident systémiques sont également leurs limites. En effet, un modèle d'accident fondé sur la théorie générale des systèmes de Bertalanffy [Bertalanffy, 1968] considérant les systèmes socio-techniques comme à l'état stable est contradictoire face à l'instabilité constante de ces systèmes par essence complexes. Dans ce cadre, l'état stable n'est qu'un cas très particulier de l'état d'un système socio-technique et ne peut pas être vu comme un état par défaut. Cette articulation a aussi permis d'apporter certaines précisions sur la notion de temps au sein des systèmes socio-techniques pour lesquels le temps peut prendre la forme d'une « flèche du temps » [Prigogine, 2001] émergeant de processus irréversibles.

La troisième et dernière articulation du chapitre 5 a eu pour ambition d'apporter un nouveau cadre de réflexion pour l'établissement d'un modèle d'accident fondé sur la théorie du chaos. Ce modèle d'accident « chaotique » ne verrait plus l'accident comme le résultat d'une chaîne d'évènements ou d'un problème de contrôle entre niveaux hiérarchiques d'un système mais comme une bifurcation d'un espace des

phases « sûr » vers un autre espace des phases pouvant être « sûr » ou « non sûr » selon la propre mémoire du système et sa capacité à répondre de façon adéquate. Ce passage reflète un changement de comportement d'un état complexe vers un état chaotique pour lequel aucune prédiction n'est envisageable. Dans ce nouveau contexte « chaotique », l'accident n'est plus vu comme un évènement mais comme un phénomène se produisant au sein d'un système. Ce phénomène caractérise le passage ou la bifurcation d'un espace des phases « sûr » vers un autre espace des phases modifiant ainsi le niveau de connaissances du système et poussant ce dernier à fournir une réponse adéquate. L'évolution même d'un système passe alors par des processus irréversibles et imprédictibles dits « phénomènes accidents » fondés sur une mémoire systémique et menant aussi bien à des phénomènes prédictibles et irréversibles dits phénomènes « impérieux » synonymes de pertes et/ou de dommages qu'à des phénomènes prédictibles et réversibles dits « incidents ». La frontière existante alors entre ce phénomène « impérieux » et ce phénomène « incident » est la sécurité représentée par un espace des phases au sein d'un attracteur regroupant l'ensemble des états d'un système libre de tous dommages ou pertes.

L'utilisation de la théorie du chaos, au travers des travaux de Prigogine et de ses structures dissipatives, permet de lire les systèmes socio-techniques non plus comme des systèmes à l'état stable, mais comme des systèmes dissipatifs se trouvant loin de l'équilibre devant sans cesse modifier leur structure grâce à leur capacité d'auto-organisation afin d'évoluer et de répondre par des processus irréversibles à toute perturbation de leur environnement. L'instabilité devient donc la « norme » et les systèmes au sens de la théorie générale des systèmes de Bertalanffy deviennent des cas très particuliers.

Ce travail de thèse a eu pour objectif de mieux comprendre l'accident au sein de systèmes socio-techniques. Cette compréhension de l'accident passe par une démarche de modélisation sur laquelle s'appuie l'analyste dans sa gestion des risques. Ainsi, plusieurs générations de modèles existent et sont le reflet d'un cadre scientifique au sein duquel ils s'inscrivent. À cet égard, les modèles d'accident ont évolué, allant des modèles dits « séquentiels » à des modèles dits « systémiques » sans jamais le remettre en question. Or, l'environnement dans lequel les systèmes socio-techniques évoluent se complexifie, montrant les limites d'un cadre aujourd'hui obsolète. Il est donc nécessaire de poser les jalons d'une nouvelle approche scientifique plus pragmatique à partir de laquelle de nouveaux modèles d'accident pourront se développer.

Bibliographie

AAIB (1994). U.S. Army Black Hawk Helicopter 87-26000 and 88-26060: Volume 1. Executive Summary: UH-60 Black Hawk Helicopter Accident, 14 April, USAF Aircraft Accident Investigation Board.

Ackoff, R.L. (1971). Towards a System of Systems Concept. Management Science 17(11): 661-671.

Alain (1951). Définition, Les Arts et les Dieux. Paris, Gallimard.

Bacon, F. (1996). Entretien avec Francis Bacon (La Quinzaine littéraire, 1971), in Marguerite Duras, Outside (1984), Gallimard, Folio.

Belanger, P. (1995). Control Engineering: A Modem Approach. Oxford, UK, Oxford University Press.

Benner, L., McDevitt, J.A. (1981). White paper No.1 System Safety Methodology. All Day Conference. Washington D.C. Chapter Of The System Safety Society, Arlington (Crystal City), VA.

Bertuglia, C.S., Vaio, F. (2005). Nonlinearity, Chaos and Complexity, The Dynamical of Natural and Social Systems, Oxford.

Bossel, H. (2007). Systems and Models, Complexity, Dynamics, Evolution, Sustainability, Books on Demand GmbH, Norderstedt, Germany.

Breugelmans, D. (2007), Novosol®: The Story of a Pluridisciplinar Step by Step Approach, Environmental Research and Development, Solvay S.A.

Carroll, J.S., Rudolph J.W., Hatakenaka S. (2002). Learning from Experience in Highhazard Organizations. Research in Organizational Behavior 24: 87-137.

Chapman.C, Ward.S (2003), Project Risk Management, Processes, Techniques and Insight. Wiley.

Checkland, P. (1999). Systems Thinking, Systems Practice, Includes a 30-Year Retrospective New York, NY, John Wiley & Sons.

Commoner, B. (1972). L'Encerclement, Paris : traduit de l'américain par G. Durnad, Editions du Seuil.

Cournot, A. (1851). Essai sur les Fondements de nos Connaissances.

Darwin, C. (1859), L'Origine des Espèces.

de Rosnay, J. (1975). Le Macroscope, Vers une Vision Globale. Le Seuil.

de Rosnay, J. (1995), L'Homme symbiotique — Regards sur le troisième millénaire. Le Seuil.

Dekker, S. (2006). The Field Guide to Understanding Human Error. Ashgate.

Depelsenaire, G. (2006). Novosol® : procédé de stabilisation pour résidus minéraux contaminés par des métaux lourds et des composés organiques, Solvay S.A.

Deschanels, J.-L. (2003). Risk Management, Modélisation de l'entreprise. Maîtrise des Risques, AFNOR.

DoD (2000). MIL-STD-882D - Standard Practice for System Safety. D. o. Defense.

Dommasch, D., O. (1962). Principles Underlying Systems Engineering. Pitman.

Dulac, N. (2007) A Framework for Dynamic Safety and Risk management Modeling in Complex Engineering Systems, MIT.

Dulac, N., Leveson, N.G. (2004). An Approach to Design for Safety in Complex Systems. INCOSE04. Toulouse, France.

Dulac, N., Leveson, N.C. (2004). Incorporating Safety in Early System Architecture Trade Studies. International System Safety Conference San Diego, CA.

Durant, D., (1979). La Systémique. Que sais-je? PUF.

Ericson II, C. A. (2005), Hazard Analysis Techniques for System Safety, John Wiley & Son, USA.

Ferry, T.S. (1988). Modern Accident Investigation and Analysis. Second Edition.New York : J.Wiley.

Forrester, J.W. (1961). Industrial Dynamics, Pegasus Communications.

Forrester, J.W. (1969). Urban Dynamics. Cambridge, MA, Productivity Press. 329

Forrester, J.W. (1972). World Dynamics. Cambridge, MA, Productivity Press.

Forrester, J.W. (1973). Confidence in Models of Social Behavior with Emphasis on System Dynamics Models, MIT.

Forrester, J.W. (1992). From the Ranch to System Dynamics: An Autobiography. In: Arthur G. Bedeian, ed., Management Laureates: A Collection of Autobiographical Essays. Volume 1 of 3. Greenwich, CT: JAI Press.

Fromentin, E. (1863) Dominique. Gallimard, 1974.

Garbolino, E., Chéry, J.P., Guarnieri, F., (2010). Modélisation Dynamique des Systèmes Industriels à Risques, Editions Tec&Doc.

Gharajedaghi, J. (2006). Systems Thinking, Managing Chaos and Complexity: A Platform for Designing Business Architecture, Butterworth-Heinemann.

Hall, A.D. (1962). A Methodology of Systems Engineering. Von Notrand Company Inc.

Hayhurst, K.J., Holloway, C.M. (2003). Second Workshop on the Investigation and Reporting of Incidents and Accidents. IRIA 2003, National Aeronautics and Space Administration Washington, DC 20546-0001, NASA/CP-2003-212642, Hampton, VA: NASA Langley Research Center.

Heinrich, H.W. (1931). Industrial Accident Prevention, A Safety Management Approach. McGraw.

Höhl, H., Ladkin, P.(1997), Analysing the 1993 Warsaw Accident With a WB-Graph, Report RVS-Occ-97-09.

Hollnagel, E., Woods, D. (1983) Cognitive Systems Engineering: New Wine In New Bottles. International Journal of Man-Machine Studies, 181 583-600 (reproduit dans International Journal of Human-Computer Studies, 1999, 51, 339-356).

Hollnagel, E. (1993). Human Rreliability Analysis: Context and Control. San Diego, California, Academic Press.

Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method. Oxford: Elsevier Science.

Hollnagel, E. (2001). Anticipating Failures: What Should Predictions be About ? In The Human Factor in System Reliability – Is Human Performance Predictable? RTO Meeting Proceedings 32, RTO-MP-32, January, Research and Technology Organization, North Atlantic Treaty Organization, Cedex, France:RTO/NATO.

Hollnagel, E. (2004). Barriers and Accident Prevention, Ashgate Publishing.

Hollnagel, E., Woods D., Leveson, N.G. (2005). Resilience Engineering: Chronicling the Emergence of Confused Consensus, Ashgate Publishing.

Hollnagel, E. (2006). Resilience – The Challenge of The Unstable. In Hollnagel, E., Woods, D. D., and Leveson, N. (2006). Resilience Engineering: Concept and Precepts. Aldershot: Ashgate.

Hollnagel, E., Woods D. (2005). Joint Cognitive Systems: Foundation of Cognitive Systems Engineering Systems. New York: Taylor&Francis.

Hopkins, A. (2000). Lessons from Longford: The Esso Gas Plant explosion. Sydney/CCH.

Ishimatsu T., Leveson N., Thomas J., Katahira M., Miyamoto Y., Nakao, H. (2010). Modeling and Hazard Analysis Using STPA, MIT, Japan Aerospace Exploration Agency.

Johnson, C., Holloway, C.M. (2004) The ESA/NASA SOHO Mission Interruption: Using the STAMP Accident Analysis Technique for a Software Related Mishap, Department of Computing Science, University of Glasgow, Scotland.

Johnson, C.J., Botting, R.M. (1999) Using Reason's Model of Organisational Accidents in Formalising Accident reports. Cognition, Technology and Work, 1, 107-118.

Johnson, C.W. (2003). The Failure of Safety-Critical Systems: A Handbook of Accident and Incident Reporting. October, Glasgow, Scotland/Glasgow University Press.

Kiel, D., Elliot, E. (1997), Chaos Theory in the Social Sciences, Foundations and Applications, Michigan Editions.

Kolmogoroff, A. (1954), The General Thing of Dynamical Systems and Classical Mechanics, International Mathematical Congress, Amsterdam.

La Porte, T.R., Paula Consolini (1991). Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations. Journal of Public Administration Research and Theory 1: 19-47.

La Porte, T.R. (1996). High Reliability Organizations: Unlikely, Demanding, and At Risk. Journal of Contingencies and Crisis Management 63(4). 330

Laracy, J.R. (2006). A System Theoretic Accident Model Applied to Biodefense, Complex System Research Lab, MIT.

Laracy, J.R. (2007), A Systemic-Theoretic Security Model for Large Scale, Complex Systems Applied to the US Air Transportation System.

Le Breton, D. (2000). Passion du Risque, Paris, Métailié, coll "mise à jour".

Le Moigne, J.L. (1977). La Théorie du Système Générale. Théorie de la modélisation, Paris, Col., Systèmes-Décisions, Presses Universitaires de France.

Le Moigne, J.L. (1999), La Modélisation des Systèmes Complexes, Dunod.

Leroy, A., Signoret, J.P. (1992). Le Risque Technologique, PUF. Que sais-je ? n° 2669.

Leplat, J. (1987). Occupational accident research and systems approach. New Technology and Human Error. K. D. Jens Rasmussen, and Jacques Leplat. New York, NY, John Wiley & Sons: 181-191.

Le Ray, J. (2006). Gérer les Risques, Pourquoi ? Comment ?. Edition AFNOR.

Leveson, N.G. (1995). Safeware: System Safety and Computers. Reading, MA, Addison-Wesley.

Leveson, N.G. (2001). Evaluating Accident Models using Recent Aerospace Accident – Part 1: Event-Base Models. Technical Report, Aeronautics and Astronautics Department, Massachusetts Institute of Technology, June 28, Cambridge, MA:MIT.

Leveson, N.G (2002). Model-Based Analysis of Socio-Technical Risk, Technical Report, Engineering Systems Division, Massachusetts Institute of Technology.

Leveson, N.G. (2003). A New Approach to Hazard Analysis for Complex Systems. International Conference of the System Safety Society. Denver, CO.

Leveson, N.G. (2003). White Paper on Approaches to Safety Engineering, MIT.

Leveson, N.G., Daouk, M., Dulac, N., Marais, K. (2003). A Systems Theoretic Approach to Safety Engineering, Aero/Astro Department, MIT.

Leveson, N.G. (2004). A New Accident Model for Engineering Safety Systems. Safety Science 42(4): 237-270.

Leveson, N.G. (2004). The Role of Software in Spacecraft Accidents. Journal of Spacecraft and Rockets 41(4): 564- 575.

Leveson, N.G., Daouk, M., Dulac, N., Marais, K. (2004). A Systems- Theoretic Approach to Safety Engineering: A Case Study MIT ESD External Symposium, Cambridge, MA.

Leveson, N.G. (2005). Safety in Integrated Systems Health Engineering and Management. Paper presented at the NASA Ames Integrated System Health engineering and Management Forum.

Leveson, N.G., Dulac, N. (2005). Risk Analysis of NASA Independent Technical Authority. Cambridge, MA, MIT. 331

Leveson, N.G., Dulac, N. (2005). Safety and Risk Driven Design in Complex Systems of Systems. NASA/AIAA Space Exploration Conference. Orlando, FL.

Leveson, N.G., Dulac, N., Marais, K., Carroll, J. (2005), Moving Beyond Normal Accidents and High Reliability Organizations: A systems Approach to Safety in Complex Systems, MA, MIT.

Leveson, N.G. (2006). A New Approach to System Safety Engineering. Cambridge, MA, Unpublished Manuscript.

Linder, B., Garcia, J., Neiman, A. (2003) Effects of Noise in Excitable Systems, phys rep.

Lorenz, E. (1963) Deterministic Non-periodic Flow. *J. Atmos. Sci.,* **20,** 130-141.

Lorenz, E. (1972) Predictability : Does the Fly of a Butterfly's Wings in Brazil Set Off a Tornado in Texas ?, American Association for the Advancement of Science.

Marais, K., Dulac, N., Leveson, .G. (2004). Beyond Normal Accidents and High Reliability Organizations: Lessons from the Space Shuttle. MIT ESD External Symposium, Cambridge, MA.

Marais, K. (2005). A New Approach to Risk Analysis With a Focus on Organizational Risk Factors. Department of Aeronautics and Astronautics. Cambridge, MA, Massachusetts Institute of Technology.

March, J.G., Sproull, L.S., Tamuz, M. (1991). Learning from Samples of One or Fewer. Organizational Science.2.

McDonnell, D., Abbott, D. (2009) What is Stochastic Resonance ? Definitions, misconceptions, debates and its relevance to biology, PLos Computational Biology.

Meadows, D.H., Meadows, D.L., Randers, J., Behrens, W.W. (1972). Limits to Growth. New York, NY, New American Library.

Meadows, D.H., Meadows, D.L., Randers, J. (1992). Beyond the Limits: Confronting Global Collapse, Envisioning A Sustainable Future. Post Mills, VT, Chelsea Green.

Meadows, D.H., Randers, J., Meadows, D.L. (2004). Limits to Growth, The 30-Year Update, EarthScan, USA.

Meadows, D. (2008), Thinking in Systems, A Primer, Edited by Diana Wright, Sustainability Institute, Chelsea Green Publishing, USA

Métais-Chastanier, B. (2010). L'accident, la technique et l'occasion. Agôn, Dossier n°2 : l'Accident.

Newton, I. (1687) Philosophae Naturalis Principia Mathematica, jussu societatis regiae ac types.

Novosol®. (2010). www.novosol.be. Solvay S.A.

Ogata, K. (1997). Modern Control Engineering. Pearson US Imports.

Ouyang, M., Hong, L., Yu, MH, Fei, Q. (2010) STAMP-Based Analysis on the Rail Accident and Accident Spreading: Taking the China-Jiaoji Accident For Example, Institute of Systems Engineering, Huazhong University and Technology, Wuham, China & Department of Civil and Environment Engineering, Rice University, TX, USA.

Parasuraman, R. (1997) Humans and Automation: Use, Misuse, Disuse, Abuse. Human Factors, 39(2), 230-253.

Paris, R., Sperber, F. (2009). Qu'est-ce que l'Auto-organisation ? www.matiererevolution.fr.

Paté-Cornell, E. M. (1990). Organizational Aspect of Engineering System Safety. Science 250.

Paté-Cornell, E. M., Dean Michael Murphy. (1996). Human and Management Factors in Probabilistic Risk Analysis: The SAM Approach and Observations From Recent Applications. Reliability Engineering and System Safety. 53

Pereira, S. J, Lee, G., Howard, J. (2006). "A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System, MDA.

Perrow, C. (1982). The President's Commission and the Normal Accident. The Accident at Three Mile Island: The Human Dimension. C. P. W. David L. Sills, and Vivien B. Shelarski Westview Press.

Perrow, C. (1984, 1999). Normal Accidents: Living with High-Risk Technologies. Princeton, NJ, Princeton University Press.

Poincaré, H. (1908). Science et Méthode.

Prigogine, I., Stenger, I. (1979). La Nouvelle Alliance, Folio Essais.

Prigogine, I., Stenger, I. (1988). Entre le Temps et l'Éternité, Librairie Arthème Fayard..

Prigogine, I. (1993). Les Lois du Chaos, Laterza, Rome.

Prigogine, I. (1996). La Fin des Certitudes, Éditions Odile Jacob.

Prigogine, I. (2001). L'Homme Devant l'Incertain, Éditions Odile Jacob.

Qureshi, Z. (2008) A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems, Australian Government, Department of Defence, Command, Control, Communication and Intelligence Division.

Qureshi, Z.H., Campbell, A. (2008), Systemic Accident Modelling of Complex Critical Socio-technical Systems in Highly Technological Organisations, Defence and System Institute, University of South Australia.

Rasmussen, J. (1983). Skill, Rules, and Knowledge; Signals, Signs and Symbols, and other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and cybernetics.

Rasmussen, J., Pejtersen, A.M., Goodstein, L.P. (1994). Cognitive Systems Engineering, Wiley-Interscience.

Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. Safety Science 27(2/3): 183-213.

Rasmussen, J., Svedung X. (2000). Proactive Risk Management in a Dynamic Society. Swedish Rescue Services Agency.

Rasmussen, J., Svedung X. (2002). Graphic Representation of Accident Scenarios: Mapping System Structure and the Causation of Accidents. Safety Science 40: 397-417.

Reason, J. (1990). Human Error. New York: Cambridge University Press.

Reason, J. (1995). A System Approach to Organizational Error. Ergonomics 38(8): 1708- 1721.

Reason, J. (1997). Managing the Risks of Organizational Accidents, Ashgate.

Rechtin, E. (1991). Systems Architecting : Creating and Building Complex Systems. Prentice Hall, 1st edition.

Roberts, K.H. (1989). New Challenges in Organizational Research: High Reliability Organizations. Industrial Crisis Quaterly

Roberts, K.H. (1990). Managing high reliability organizations. California Management Review 32(4): 101-114.

Roberts, K.H. (1990). Some characteristics of one type of high reliability organization. Organization Science 1(2): 160-176.

Rochlin, G. I., La Porte, T.R., Roberts, K.H. (1987). The Self-Designing High Reliability Organization, Naval War College Review.

Ruyer, R. (1930). Esquisse d'une philosophie de la Structure, Thèse Principale présentée à la Faculté des lettres de l'Université de Paris. F.Alcan.

Sagan, S.D. (1993). The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton, NJ, Princeton University Press.

Sagan, S.D. (2004). The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security. Risk Analysis 24(4): 935-946.

335

Senders, J.W., Moray, N.P. (1991). Human Error: Cause, prediction, and Reduction. Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Senge, P.M. (2006). The Fifth Discipline: The Art and Practice of the Learning Organization. New York, NY, Doubleday Currency.

Setiadi, R., Kom, S. (2006), STAMP Accident Model for Safety Engineering: A Critical Analysis, M. SoftSysEng.

Shrivastava, P. (1992). Bhopal : Anatomy of a Crisis. Second Edition, London: Paul Chapman.

Skelt, S. (2002). Methods for Accident Analysis. Report No. ROSS (NTNU) 2000208, Norwegian University of Science and Technology, Trondhein: NTNU.

Sterman, J.D. (2000). Business Dynamics: Systems Thinking and Modeling for a Complex World. Boston, MA, Irwin McGraw-Hill.

Strauch, B. (2002). Investigating Human Error : Incidents, Accidents, and Complex Systems, Ashgate.

Stringfellow, M., Owens, B., Leveson, N., Ingham, M., Weiss, K. (2007). Safety Driven Model Based, System Engineering Methodology, MIT.

Thom, R., (1991), Prédire n'est pas Expliqué, Editions Ednet.

Trist, E.L., Bamforth, K.W. (1951) Some Social and Psychological Consequences of The Longwall Method of Coal-Getting. Human Relations, 4,3-39.

US-EPA (2005), Contaminated Sediment Remediation Guidance Hazardous Waste Site.

Vaughan, D. (1996). The Challenger Launch Decision: Risky Technology, Culture, And Deviance at NASA. Chicago, II, University of Chicago Press.

Virilio, P. (2005). L'Accident Originel, Paris, Galilée.

von Bertalanffy, L. (1968). General system theory. New York, NY,

Wasserman, S., Faust, K. (1994). Social Networks Analysis: Methods and Applications. Cambridge, UK, Cambridge University Press.

Weinberg, G.M. (1975). An Introduction to General System Thinking, NY, John Willey & Sons.

Weick, K.E. (1987). Organizational Culture as a Source of High Reliability. California Management Review(Winter): 112-117.

Weick, K.E., Roberts, K.H. (1993). Collective Mind in Organizations: Heedful Interrelating on Flight Decks. Administrative Science Quarterly 38(3): 357-381.

Weick, K.E., Sutcliffe, K., Obstfeld, D. (1999). Organizing for High Reliability. Research in Organizational Behavior 21: 81-123.

Weiner, N. (1948). Cybernetics, Cambridge, MIT Press, and New York: J Wiley.

Weiner, N. (1986). Human use of Human Being: Cybernetics and Society, Avon.

Woods, D.D., Johannesen, L., Sarter, N.B (1994). Behind Human Error: Cognitive Systems, Computers and Hindsight. SOAR Report 94-01, Wright-Patterson Air Force Base, Ohio: CSERIAC.

Index des Illustrations

Index

W

Z

Contribution à l'étude du modèle d'accident systémique STAMP

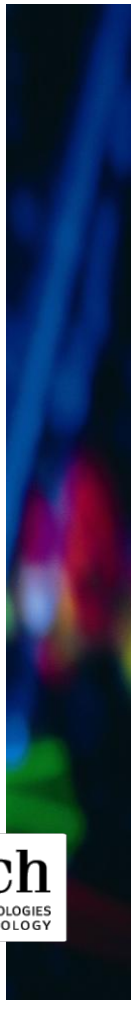
RESUME : Véritable outil de compréhension des causes et des conséquences d'événements dommageables voire catastrophiques, les modèles d'accident ont pris une place essentielle au cœur des démarches d'enquêtes-accident et/ou d'évaluations des risques au sein des systèmes socio-techniques. Leur efficacité n'est plus à prouver et nombreuses sont les organisations les utilisant aux fins de répondre à un besoin de sécurité et à des exigences de performances et de progrès. De nombreux modèles d'accident ont donc été développés. Fondés originellement sur le principe de représentations d'une chaîne d'événements reliée par des relations de causes à effets, les modèles contemporains s'appuient désormais, pour une minorité encore, sur la théorie des systèmes et la théorie du contrôle, favorisant ainsi une analyse systémique et une vision holistique des accidents et des catastrophes. Parmi les démarches de modélisation les plus récentes et abouties, le modèle d'accident systémique appelé STAMP (System-Theoretic Accident Modeling and Processes), développé au sein du Massachusetts Institute of Technology, et se fondant sur les concepts de « contrainte », de « structure » et de « modèle de processus » a été retenu dans le cadre de cette thèse. Ce modèle pose comme hypothèse que les accidents résultent d'un contrôle inefficace et inadéquat de la structure d'un système socio-technique le conduisant et le condamnant ainsi à migrer d'un état « sûr » vers un état accidentel. La thèse se fixe trois objectifs. Le premier vise à s'approprier les fondements épistémologiques, théoriques et méthodologiques sous jacents au modèle STAMP. Le deuxième consiste en la mise en œuvre effective du modèle dans le cadre de l'évaluation des risques d'un procédé industriel innovant de dépollution de sédiments contaminés. Le troisième ambitionne à apprécier les apports et les limites du modèle et de proposer au regard des limites repérées des propositions d'amélioration tant au plan théorique que méthodologique.

Mots clés : accident, modèle d'accident, théorie des systèmes, théorie du contrôle, modèle STAMP, risque, dépollution, sédiments contaminés, théorie du chaos.

Contribution to the study of STAMP model

ABSTRACT: Real tool for understanding the causes and consequences of damaging or catastrophic events, the models of accident took place at the heart of critical approaches to accident investigations, and / or risk assessments within the socio-technical systems. Their effectiveness has been proven and many organizations are using them for answering a need for safety and performance requirements and progress. Many models of accident have been developed. Originally based on the principle of representation of a chain of events linked by cause and effect relationships, contemporary models are now based, for a minority even on systems theory and control theory, thus promoting systems analysis and a holistic view of accidents and disasters. Among latest modelling approaches, systemic accident model called STAMP (System-Theoretic Accident Modeling and Processes), developed at the Massachusetts Institute of Technology, and based on the concepts of "constraint", "structure" and "Model of process" was chosen in the framework of this thesis. This model assumes that accidents result from inadequate and ineffective control of the structure of a socio-technical system leading them to an accidental state. The thesis has three objectives. The first is to capture the epistemological, theoretical and methodological fundamentals underlying the STAMP. The second is the effective implementation of the model in the context of risk assessment of an innovative industrial process to clean up contaminated sediments. The third aims to assess the contributions and limitations of the model and propose with regard to the limits identified proposals to improve both the theoretical and methodological aspects.

Keywords : accident, model of accident, system theory, control theory, STAMP, hazard, contaminated sediments, chaos theory.



MINES ParisTech

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY